UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Sistema seguro de monitoreo de variables utilizando redes de sensores inalámbricos.

Trabajo Fin de Máster

presentado por: Diaz Suárez, Ricardo

Director/a: Cuquejo Mira Juan

Ciudad: Madrid
Fecha: 2017

Resumen

En este proyecto de investigación se presenta el desarrollo de un sistema seguro para el monitoreo de variables ambientales. Para realizar este sistema primero se elaboró un estado del arte para conocer las diversas vulnerabilidades presentes en las redes de sensores inalámbricos, seguidamente se desarrolló una red de sensores para monitorizar la temperatura utilizando radios XBEE. Los sensores fueron configurados para que las transmisiones estén cifradas utilizando AES. La información proveniente de los sensores es registrada, cifrada y transmitida hacia un servidor remoto utilizando una conexión segura TLS por un software desarrollado en node.js. La información enviada por los sensores es visualizada en un aplicativo web desarrollado en php. Para la validación de su funcionamiento se realizaron pruebas de monitoreo de red utilizando la plataforma zigbee MC1322x y el analizador de paquetes wireshark, donde se comprobó que la transmisión es cifrada desde el nodo sensor hasta el servidor destino.

Palabras Clave: sensor, cifrar, nodejs, TLS, servidor.

Abstract

This research project presents the development of a safe system for the monitoring of environmental variables. In order to perform this system, a state of the art was elaborated to know the various vulnerabilities present in the networks of wireless sensors, followed by the development of a network of sensors to monitor the temperature using XBEE radios. The sensors were configured so that the transmissions are encrypted using AES, the information from the sensors is recorded, encrypted and transmitted to a remote server using a secure TLS connection by software developed in node.js. The information sent by the sensors is displayed in a web application developed in php. For the validation of its operation, network monitoring tests were performed using the MC1322x zigbee platform and the wireshark sniffer, where it was verified that the transmission is encrypted from the sensor node to the destination server.

Keywords: sensor, cipher, nodejs, TLS, server

TABLA DE CONTENIDO

Contenido

Índice de Figuras.

Índice de Tablas

1. Introducción.

1.1 Motivación.

El desarrollo actual de las redes de sensores inalámbricos está permitiendo el despliegue de un sin número de aplicaciones en diversas áreas de la ingeniería. Algunos de estos desarrollos se encuentran enfocados en el monitoreo de variables y otros están redireccionados al control de las variables o automatización de procesos. Sin embargo las comunicaciones que se establecen desde los nodos de sensores inalámbricos hasta las centrales de monitoreo en gran diversidad de escenarios carecen de los mecanismos de seguridad que garanticen la confiabilidad e integridad de la información obtenida por los sensores. Esta problemática puede afectar en la producción de diversas industrias que utilizan las redes de sensores inalámbricos para el monitoreo de variables críticas en sus procesos debido a las diferentes vulnerabilidades que se pueden encontrar por un delincuente informático.

Considerando la deficiencia presente en el mecanismo de transmisión de acceso al medio de los nodos inalámbricos y algunos vectores de ataques para las redes de sensores inalámbricos donde un nodo presente en la red puede suplantar a otros pudiendo enviar datos de forma errónea, además el canal de comunicación es no guiado lo cual involucra que puedan existir nodos *sniffer* (nodos que monitorean los paquetes que viajan en la red) los cuales pueden escuchar las comunicaciones considerando que las transmisiones realizadas por los nodos se realizan en texto plano. Teniendo en cuenta estos aspectos descritos anteriormente en cuanto a las vulnerabilidades presentes en las redes de sensores inalámbricos se deben implementar mecanismos para garantizar la seguridad en la información tales como el cifrado de los datos entre otros aspectos que permitan garantizar la seguridad en la información.

La información proveniente de las redes de sensores inalámbricos es enviada a un concentrador o Gateway el cual envía la información generalmente por una red TCP/IP a una base de datos remota para su posterior visualización y procesamiento que generalmente se realiza desde un aplicativo WEB. En algunos casos se utiliza un ordenador como concentrador o un sistema embebido (raspberry, bananaPi, Xbee Gateway, entre otros), los cuales generalmente envían la información sin cifrarla, lo que constituye en una vulnerabilidad crítica del sistema.

1.2 Planteamiento del trabajo.

Para solventar esta problemática descrita anteriormente se deben proveer mecanismos que permitan la integridad, confidencialidad y disponibilidad de la información proveniente de una red de sensores inalámbricos. Para solucionar esto se propone desarrollar un sistema de monitoreo seguro utilizando redes de sensores inalámbricos. Para cumplir este objetivo se desarrollará una solución tecnológica para la transmisión de forma segura de la información registrada por una red de sensores inalámbricos hacia una base de datos alojada en un *hosting* remoto. Para realizar este procedimiento, primero se propone una revisión bibliográfica de las vulnerabilidades presentes en las redes de sensores inalámbricos, seguidamente se deberá elaborar una red de sensores inalámbricos y analizar las transmisiones con un *sniffer* las lecturas de los datos transmitidos dentro de la red de sensores para conocer la estructura de las tramas. Seguidamente se propone realizar la configuración del mecanismo de cifrado para la transmisión de la información utilizando el algoritmo de AES. Posteriormente esta información es llevada hacia un nodo Gateway o concentrador donde se elaborara un aplicativo software utilizando el lenguaje de programación Javascript. Este se encargará de realizar la lectura y el proceso de cifrado. A continuación esta información deberá ser enviada hacia un *hosting* con una conexión segura utilizando TLS. En el hosting se encuentra un aplicativo web que se desarrollará en php el cual realizará el proceso de descifrado, almacenamiento de los datos en postgresql y la visualización de los datos mediante una interfaz gráfica. En cada una de las fases de desarrollo se deberán realizar pruebas tanto con un *hosting* local como en un *hosting* remoto.

1.2.1 Objetivo General

- Desarrollar un sistema de monitoreo seguro utilizando una red de sensores inalámbricos.

1.2.2 Objetivos específicos.

- Construir una red de sensores para el monitoreo de variables ambientales donde la información se transmita de forma cifrada.

- Desarrollar un aplicativo software en javascript utilizando la metodología S-SDLC para la lectura y transmisión de la información cifrada.

- Diseñar una página WEB para la lectura y visualización de los datos de las variables ambientales medidas.

1.3 Estructura de capítulos.

La estructura del libro se describe a continuación.

En el segundo capítulo se presenta una contextualización de las redes de sensores inalámbricos, características del estándar IEEE802.15.4 y un estado del arte de la seguridad en redes de sensores inalámbricos donde se describen diversos vectores de ataque, vulnerabilidades y mecanismos de seguridad presentes en las redes de sensores inalámbricos.

En el tercer capítulo se describe el desarrollo de una red de sensores utilizando radios XBEE, donde se analiza con un *sniffer* las vulnerabilidades de las tramas. Seguidamente se presenta la configuración de los XBEE para él envío de las tramas cifradas. También se presenta el desarrollo del aplicativo software utilizando S-SDLC en javascript que se ejecuta sobre node.js en el ordenador o Gateway y realiza el proceso de lectura de los datos proveniente del nodo XBEE coordinador. Además cifra estos datos utilizando AES y los envía por una conexión TLS por la red inalámbrica local hacia un *hosting* remoto. Las pruebas se realizaron primero considerando un servidor local y seguidamente con el *hosting* remoto. Para las pruebas con el servidor local se generaron los certificados utilizando la librería OPENSSL y para el servidor remoto los certificados fueron adquiridos con el *hosting* el cual se gestiona utilizando el CPANEL. Por último, se elaboró un aplicativo web en php que descifra y permite la visualización de los datos registrado por el sensor. En el cuarto capítulo se presentaran las respectivas conclusiones.

2. Contexto y estado del arte

2.1 Redes Inalámbricas de Sensores (WSN)

Las redes de sensores inalámbricos están constituidas generalmente por nodos de sensores con recursos hardware con bajas prestaciones que les permiten realizar procesos de sensado de variables, control de actuadores y transmisión de información. Con este tipo de dispositivos se pueden implementar redes *ad-hoc* sin ser necesario tener una estructura física preestablecida ni una administración central. Estas redes tienen diversidad de aplicaciones en diversos tipos de ambientes ya sea en aplicaciones industriales, domóticos, ambientales, agrarios, telemedicina entre otros. Entre las principales características de los nodos se encuentran: su facilidad en el despliegue a gran escala, su autoconfigurabilidad y el bajo costo. (Roberto Fernández Martínez, 2009)

Este tipo de redes permiten que las variables medidas o monitorizadas por la red de sensores puedan ser transmitidas a la nube desde un *gateway* ya sea por redes cableadas o inalámbricas utilizando protocolos TCP/IP. A continuación en la figura 1 se presenta una topología básica de las redes de sensores inalámbricos la cual está compuesta por un grupo de nodos que operan bajo el estándar IEEE802.15.4. Estos nodos envían la información a un concentrador o Gateway el cual utiliza diferentes tecnologías de comunicación (Ethernet, Wi-Fi, GPRS, entre otros) los cuales permiten la transmisión la información hacia la nube para el almacenamiento remoto de la información adquirida por los sensores.

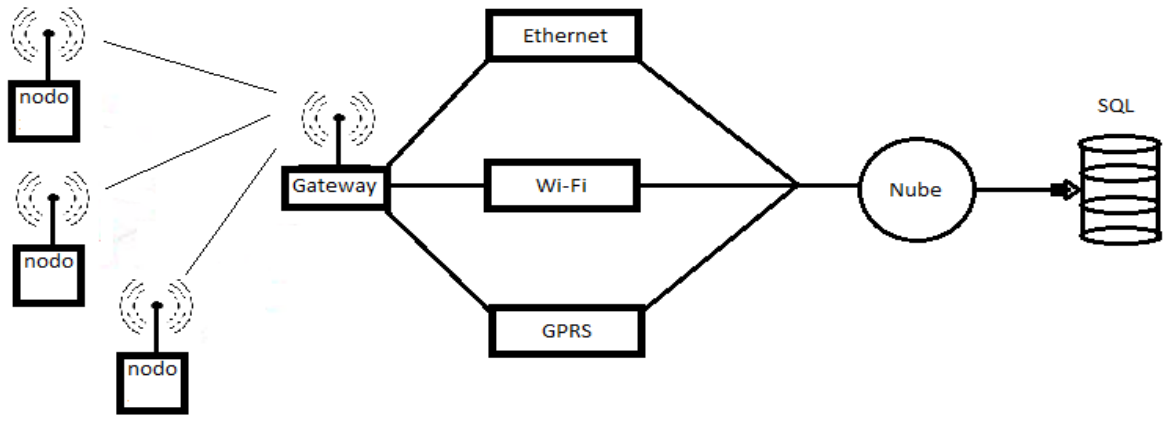


Figura 1. Red de sensores inalámbricos y componentes de conectividad.

2.2 Componente de un nodo sensor.

Cada nodo que constituye un sensor inalámbrico de comunicación se considera como un pequeño ordenador el cual tiene periféricos de entrada y salida, conversores análogos

digitales, un *transceiver* que permite la comunicación del dispositivo con otro nodo o la puerta de enlace, una unidad central de procesamiento, un sistema de almacenamiento, un sistema de alimentación en algunos casos tiene sistemas de posicionamiento global. A continuación en la figura 2 se presentan los componentes de nodo sensor. (Roberto Fernández Martínez, 2009) (Carlos Garcia Arano, 2010) (Diana Milena Archila Córdoba, 2013)

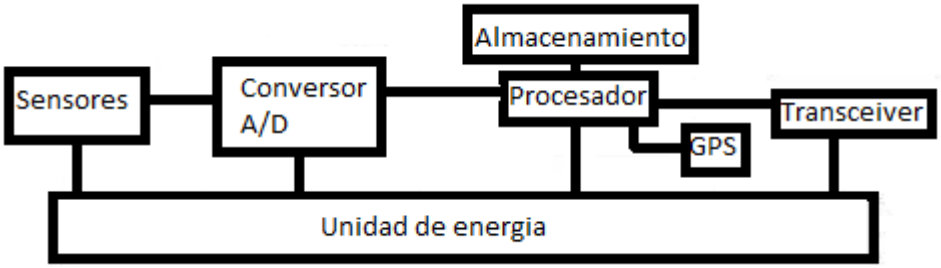


Figura 2. Componentes del nodo sensor.

2.3 Aplicaciones de las redes de sensores

El mercado del monitoreo de variables utilizando WSN ha aumentado circunstancialmente debido a las aplicaciones de *big data, IoT (internet of things)*, los bajos costos de esta tecnología y un sin número de aplicaciones que están solicitando un registro de eventos constante. Entre las aplicaciones de las redes de sensores se cuentan: En el medio ambiente, instalaciones de seguridad, monitoreo de tráfico, medicina, domótica e inmótica entre otros. A continuación se describe de una forma más detallada algunas de las aplicaciones donde se implementan las redes de sensores inalámbricos. (Roberto Fernández Martínez, 2009) (Suescún, 2009)

Medio ambiente: En el monitoreo ambiental sería imposible tener datos fiables sin el despliegue de una red de sensores, ya que este tipo de redes ofrecen gran cobertura en el monitoreo de temperatura, humedad, fuego, presencia de gases y actividad sísmica. Esto permite tener un mejor control del comportamiento de los microclimas. También se usan en ambientes industriales y en grandes fábricas las cuales deben monitorizar sus procesos para generar productos de alta calidad.

Instalaciones de seguridad: Para los entornos de seguridad con el despliegue de una red de sensores se puede realizar un monitoreo en grandes áreas que sería imposible utilizando cámaras de alta resolución.

Monitoreo de tráfico: Consiste en realizar un despliegue de sensores sobre carreteras para conocer el tráfico de vehículos.

Medicina: Sirve para ofrecer servicios de telemedicina donde se puede monitorizar de forma permanente y remota variables vitales tales como la frecuencia cardiaca, temperatura corporal, presión arterial, frecuencia respiratoria.

Domótica e inmótica: En el ámbito de la domótica se emplea para tener un sistema de control de encendido de luces y el monitoreo de concentración de gases, entre otros aspectos.

Estructuras: Dentro de este ámbito se realizan mediciones de vibración sobre puentes y edificaciones.

Monitoreo Industrial: Se realiza el monitoreo de la maquinaria y el ruido presente en estas.

Monitoreo de procesos: En esta parte se monitorea la velocidad, aceleración y dirección los procesos.

Seguimiento de activos: Identificación y seguimiento de objetos. (Diana Milena Archila Córdoba, 2013)

En la figura 3 se presenta el mercado de las redes de sensores y su adopción en diversas industrias.

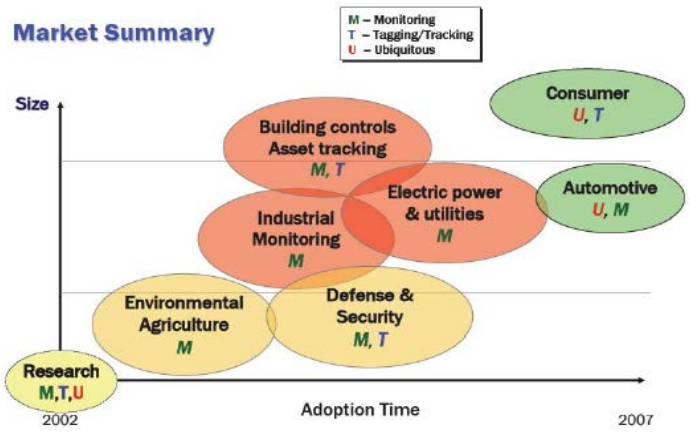


Figura 3 . Mercado para las redes de sensores. *(Roberto Fernández Martínez, 2009)*

2.4 Reseña histórica de las redes de sensores inalámbricos.

El desarrollo de las redes de sensores se inició con aplicaciones militares, donde la primera red de este tipo se llamó *Sound Surveillance System*, la cual consistía en el despliegue de sensores acústicos diseñados para percibir los sonidos que emitían los submarinos nucleares

Rusos en la guerra fría. Otra aplicación fue el despliegue en EEUU de una red de sensores constituidos por radares sobre aeronaves. Estos tipos de aplicaciones después se utilizaron en la sísmica y biología. (Silicon Laboratories, 2013)

El procesamiento en las primeras redes de sensores se realizaba de forma jerárquica antes de llegarle la información al usuario final. Las investigaciones fuertes realizadas sobre redes de sensores inalámbricos se iniciaron con el proyecto DSN (*Distributed Sensor Networks*), cuando DARPA (*Defense Advance Research Projects Agency*) quiso implementar el método de comunicación ARPANET sobre una red de sensores. Esta prueba fue realizada sobre una red de sensores que se encontraban espacialmente distribuidos, donde cada nodo interactuaba con los otros pero cada uno era totalmente autónomo. Seguidamente se comenzaron a generar los primeros sistemas operativos para los nodos tales como Accent y lenguajes de programación como SPLICE. (Silicon Laboratories, 2013) (ITU-T, 2014)

Dentro de los años 80 y 90 las redes de sensores tuvieron gran auge en las aplicaciones militares perfeccionándose en la detección de francotiradores, aunque todavía faltaban algunos años para que se iniciara su miniaturización. En década pasada se generaron diversos avances para las redes de sensores en cuanto al tamaño, autonomía, seguridad y costo lo cual permitió hacer aplicaciones en diversas ramas de la ingeniería. (ITU-T, 2014)

2.5 Diseño de una red de sensores inalámbricos

En el diseño de una red de sensores se deben tener presente los siguientes aspectos para poder garantizar su buen funcionamiento. (Perez Juan, 2014) (Carlos Garcia Arano, 2010) (Roberto Fernández Martínez, 2009)

- **Tolerancia a fallos:** Los nodos de sensores pueden tener fallas por falta de energía, interferencia electromagnética, daño físico o bloqueo del firmware. Un fallo no puede comprometer el funcionamiento de la red de sensores.
- **Escalabilidad**: La red de sensores debe permitir el incremento del número de nodos (cientos y miles) sin tener inconvenientes dentro de la red.
- **Costes de producción:** El costo de cada uno de los sensores es crucial para la elaboración de una red de sensores.
- **Limitaciones en hardware:** Cada nodo está constituido por una unidad de sensado, el cual está integrado por un conversor analógico digital, un dispositivo sensor, una

unidad de procesamiento, un módulo de comunicación *transceiver* y un módulo de alimentación. Alguno de estos cuentan con sistemas de posicionamiento global.

- **Topología:** La topología se describe en tres fases. Pre-despliegue, despliegue y postdespliegue de nodos adicionales.

- **Entorno:** Los nodos pueden ser desplegados cerca de la variable a registrar. Estos nodos pueden trabajar en zonas remotas, ya que pueden integrar con otras tecnologías para transmitir la información en largas distancias.

- **Medios de transmisión**: En las redes de sensores multisalto, los nodos generalmente está conectados a un canal de comunicación inalámbrico, algunos trabajan con enlaces ópticos.

- **Consumo energético:** Los nodos son alimentados generalmente por baterías, dependiendo del tamaño de la batería se relaciona la autonomía de los nodos.

2.6 Tipos de nodos.

A continuación se describen los diferentes tipos de nodos presentes en las redes de sensores inalámbricos.

Nodo final: Dentro de su funcionalidad tiene las características para poderse comunicar con un nodo router o coordinador, pero no tiene las capacidades de transmitir la información a otro tipo de dispositivos. (Perez Juan, 2014)

Nodo Router: En su funcionalidad permite la ejecución de código de usuario. Además este dispositivo puede interconectar los dispositivos que están separados de la topología de red. (Perez Juan, 2014)

Nodo Coordinador: Este nodo tiene la funcionalidad de controlar la red y definir la forma en que los dispositivos se deben conectar entre ellos, en cualquier red de sensores debe existir por lo menos uno de estos tipos de nodos. (Perez Juan, 2014)

2.6.1 Arquitectura de la red de sensores inalámbricos.

En la arquitectura se contempla la medición de un grupo de variables. Dicha información es transmitida de forma digital desde el nodo sensor hacia el nodo router o nodo coordinador el cual transmite la información hacia un *gateway* o puerta de enlace, el cual se comunica de

forma cableada o inalámbrica a una estación base donde pueden ser almacenados los datos. En la figura 4 se presenta la arquitectura de una red de sensores inalámbricos contemplando diversos tipos de nodos. (Carbajal, 2012)

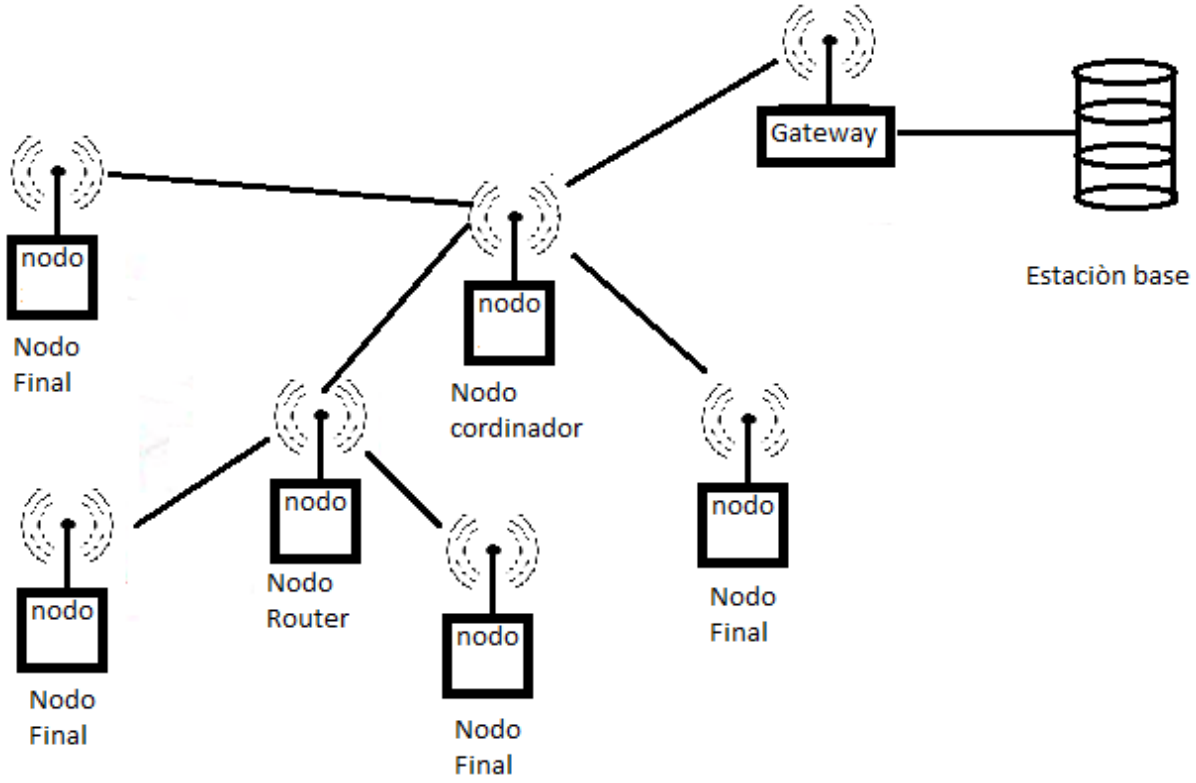


Figura 4. Arquitectura de una red de sensores inalámbricos.

2.7 Características de las redes de sensores.

2.7.1 Topología.

Las redes de sensores inalámbricos generalmente toman diferentes topologías físicas. Debido a esto se deben configurar los nodos de tal forma que se tengan su autonomía y que de esta forma se evite tener una intervención física sobre estos dispositivos. Generalmente esto se realiza utilizando protocolos de comunicación distribuidos. (Roberto Fernández Martínez, 2009)

Topología en estrella.

Para la topología en estrella se establece la comunicación entre el nodo coordinador FDD (dispositivo de funcionalidad completa) y los nodos finales RFD (Dispositivo de funcionalidad reducida). En este tipo de topología el nodo central define un ID (Identificador) para establecer

el canal de comunicación con los demás nodos pertenecientes a la red. (Roberto Fernández Martínez, 2009)

Topología tipo malla

Todos los nodos de la red tienen características de coordinador para el enrutamiento de los datos donde se utilizan diversos protocolos para el encaminamiento AODV (*Ad Hoc On- Deman distance vector*) y DYMO (*Dynamic Manet On-Demand*) de los datos. Esto permite hacer el despliegue de la red en grandes espacios, donde cada nodo se comunica con otro mientras se encuentra en la misma área de cobertura. (Roberto Fernández Martínez, 2009)

Topología hibrida

Es considerado una combinación entre nodos FFD y RFD donde se integra la comunicación entre varios nodos coordinadores donde cada uno se conecta con dispositivos finales en topología árbol. (Roberto Fernández Martínez, 2009)

2.7.2 Consumo de energía.

Los nodos utilizados en las redes de sensores inalámbricos tienen características de bajo consumo de potencia, además tienen modos de configuración donde el nodo entra en modo *sleep*, lo que les permite tener tiempos de autonomía elevados. Algunos de estos sistemas contemplan un sistema de alimentación fotovoltaica para su autonomía. (Roberto Fernández Martínez, 2009)

2.8 Estándar IEEE 802.15.4 (Zigbee)

A continuación se presentan las principales características del estándar que describen el comportamiento de la red de sensores inalámbricos.

El estándar IEEE 802.15.4 surge a la escasez de estándares inalámbricos de baja tasa de transmisión y bajo consumo de potencia para las redes de sensores. Los estándares disponibles como Bluetooth, Wi-Fi, Wimax están definidos para manejar elevados anchos de banda, con diferentes tipos de cobertura PAN, LAN, WAN, además tienen elevado consumo de potencia.

Los diferentes fabricantes de sensores inalámbricos integraban sus propios protocolos de comunicación lo cual generó gran incompatibilidad entre los diferentes fabricantes, esto incentivó la generación del estándar.

El estándar IEEE802.15.4 define las características básicas de la capa física y del control de acceso al medio. El estándar ZigBee complementa al estándar ofreciendo funciones de la capa de red que permite gestionar las características de enrutamiento.

2.8.1 Tipos de nodos sensores inalámbricos.

Nodo FFD: Son los nodos (Coordinadores y enrutadores) que tienen la capacidad de organizar y coordinar el acceso al medio de otros dispositivos que hacen parte la misma red. Estos tipos de nodos se consideran como los nodos centrales de la red. (Jorge Pablo Dignani, 2011)

Nodo RFD: Se consideran como los nodos finales (*end device*) de red. Entre sus principales características se encuentran su bajo consumo de potencia comparado con el FFD y que las capacidades de enrutamiento son limitadas. (Jorge Pablo Dignani, 2011)

2.8.2 Capa Física del 802.15.4

La capa física está separada en dos subcapas: *PHY data service* y *PHY management*, las cuales son las encargadas de transmitir y recibir señales utilizando el canal de comunicación de radiofrecuencia.

Entre las principales características de la capa física están el *transceiver*, la selección del canal de comunicación, el detector del canal, detector de energía y la estimación de claridad del canal. La técnica de acceso al medio que utiliza es CSMA-CA (*Carrier Sense Multiple Access – Collision Avoindance*). Las frecuencias de operación son las bandas no licenciadas (868Mhz, 915Mhz, 2450Mhz) utilizando como técnica de modulación *direct sequence spread spectrum,* la cual es una técnica de espectro ensanchado para modular la información. Las velocidades de transmisión que manejan dentro del estándar son 20, 40, 250Kbps. (IEEE Standards Associations, 2015)

Dentro del estándar el paquete de la capa física se llama (*Physical Layer convergence protocol*) PLCP protocolo unidad de dato, la cual se encuentra compuesta en tres segmentos los cuales serán descritos a continuación. (IEEE Standards Associations, 2015) (IEEE Standards Associations, 2015)

SHR (Encabezado de sincronización): Permite realizar una sincronización del arribo del paquete donde indica el inicio y el final del paquete. (IEEE Standards Associations, 2015)

PHR (Cabecera física): Este campo tiene la información del tamaño del paquete. (IEEE Standards Associations, 2015)

PSDU (Unidad de dato del servicio físico): En este campo lleva la información del paquete. (IEEE Standards Associations, 2015)

2.8.3 La capa MAC del 802.15.4

Esta capa proporciona *MAC data service* y *MAC management service*, los cuales proveen los mecanismos en recepción y transmisión de la tramas MPDU sobre la capa física. Entre las principales características de esta capa se tiene: la generación de *beacons*, los mecanismos de acceso al medio CSMA-CA, asociación y desasociación a la red de área personal. Funciones de seguridad (Cifrado AES) y calidad de servicio. (IEEE Standards Associations, 2015)

Dentro del estándar IEEE802.15.4 se encuentran tres formas de transmitir datos, la primera de estas es transmitir datos utilizando *beacons*, otra forma es transmitir datos sin *beacons*, y la otra es transmitir datos considerando *beacons* con un tiempo de acceso al canal de comunicación garantizado. (IEEE Standards Associations, 2015)

La transmisión con *beacons* está orientada a la red tipo estrella donde el nodo coordinador es el encargado de transmitir los *beacons* cada cierto tiempo a los diversos nodos de la red para que los nodos que hacen parte de la red se puedan sincronizar. Esto permite que se establezca una supertrama formada por slots que generan un periodo de contención para que los dispositivos puedan transmitir de forma ordenada. (IEEE Standards Associations, 2015)

Cuando se realiza la transmisión sin *beacons* esto se utiliza para la conexión *peer to peer* donde cada nodo espera un tiempo aleatorio y una ventana *backoff* donde no percibe una transmisión para iniciar la transmisión. (IEEE Standards Associations, 2015)

En el modo de transmisión utilizando *beacons* y un tiempo de acceso garantizado, permite tener una latencia determinista, el GTS (*Guaranted Time slot*) se encuentra definido dentro de un periodo libre de contienda. (IEEE Standards Associations, 2015)

2.8.3.1 Características de acceso al medio del estándar IEEE802.15.4.

El estándar está definido para que su funcionamiento se realice en entornos de comunicación hostiles y que compartan el medio con otras tecnologías de comunicación tales como Wi-Fi y bluetooth.

El mecanismo de transmisión utilizado CSMA-CA (*Carrier sense multiple Access collision avoidance)*, utiliza la detección de portadora como mecanismo para evitar las colisiones cuando se accede al canal de comunicación. (IEEE Standards Associations, 2015) (Carlos Garcia Arano, 2010)

Otras características de este mecanismo de transmisión dentro del estándar se describen a continuación:

Confirmación de arribo de paquetes utilizando paquetes de acuse de recibo ACK.

Verificación de las tramas de datos utilizando códigos de redundancia cíclica. Se utiliza un polinomio de generador de 16 para obtener redundancia donde se puede comparar el CRC enviado con el que se está calculando en el destino para la verificación de los datos que fueron enviados. (IEEE Standards Associations, 2015) (Carlos Garcia Arano, 2010)

El consumo de energía se realiza a través de baterías lo cual limita su funcionalidad. Esta se encuentra sujeta a los modos de transmisión que tenga implementado *sleep mode* y el tipo de monitoreo de las variables.

2.9 Seguridad estándar IEEE802.15.4

Las redes inalámbricas elaboradas con este estándar tienen las mismas vulnerabilidades de las otras redes *AD-HOC* tales como la escucha por nodos intrusos pasivos de las comunicaciones establecidas por los nodos y la alteración por acceso físico a los nodos. Las limitaciones del hardware tanto en almacenamiento como en procesamiento limitan la selección de algoritmos de cifrado, protocolos y el diseño de la arquitectura de seguridad para poder establecer y mantener una relación de confianza entre los nodos debe realizarse con cuidado. Otra limitante es el tiempo de vida de la alimentación y las limitaciones del costo pueden introducirle limitaciones a la sobrecarga en la seguridad. (IEEE Standards Associations, 2015)

Se considera que los mecanismos de cifrado dentro del estándar están soportados por procesos en las capas superiores y que el mantenimiento y establecimiento de las claves se describe que se encuentran fuera del estándar.

Sin embargo se describe dentro del estándar que el mecanismo de cifrado permite proveer una particular combinación de los siguientes servicios de seguridad.

Confidencialidad de los datos: Asegura que la información trasmitida solo es divulgada a las partes interesadas. (IEEE Standards Associations, 2015)

Autenticación de los datos: Asegura que la información enviada no ha sido alterada o modificada en el proceso de transmisión. (IEEE Standards Associations, 2015)

Protección a duplicados: Asegura que la información duplicada puede ser detectada. (IEEE Standards Associations, 2015)

El cifrado es realizado *frame-frame* lo cual permite diferentes niveles de autenticación y permite minimizar las cabeceras de seguridad dentro de los *frames* que son trasmitidos donde es requerido y para datos opcionales de confidencialidad. Para la protección por cifrado de *frame* utiliza intercambio de claves dentro de un par de dispositivos o dentro de un grupo de dispositivos, de esta forma provee algo de flexibilidad entre el almacenamiento y el costo de mantenimiento de las claves comparado con la protección que provee el cifrado. Si existe una clave de grupo y esta es utilizada para comunicaciones punto a punto, esta solo provee contra atacantes externos y no contra nodos potenciales maliciosos dentro de la clave que se intercambió dentro del grupo. (IEEE Standards Associations, 2015)

Para la parte de seguridad, implementa clave simétrica mediante el estándar de encriptación AES. El manejo y la gestión de las claves se realizan en las capas superiores.

El estándar IEEE802.15.4 establece aspectos relevantes para garantizar la autenticación de los nodos de comunicación evitando que cualquier nodo intruso pueda vulnerarla. Además el estándar define el tipo de algoritmo de cifrado que debe utilizarse para las operaciones de criptografía.

La mayoría de los ataques se consideran que provienen desde la parte interna de la red donde el nodo intruso tiene acceso lógico a la red. Un ataque proveniente desde afuera de la red se puede considerar casi imposible, por lo tanto se considera que para evitar varios de los ataques se debe evitar que un nodo intruso se asocie o entre a la red establecida.

Existen diferencias entre la versión 2003 y 2006 descritas para el estándar IEEE802.15.4 en cuanto a la información para gestionar la seguridad.

La seguridad está dada a partir de cifrado simétrico el cual permite establecer la confiabilidad e integridad de las comunicaciones. El estándar define a AES (*Advance encryption standard*) con una longitud de clave de 128btis, donde este algoritmo es utilizado tanto para cifrar como validar la información. Este procedimiento lo realiza utilizando un código de integridad o código de autenticación del mensaje, al añadirse al final del mensaje se busca que se tenga integridad en la información que se esté transmitiendo (la cabecera MAC y los datos o *payload*) además

ayuda a garantizar que el emisor dice ser quien es. Al recibir una trama de un nodo que no es confiable, el código de integridad no debe coincidir al haberse generado con una clave diferente. (IEEE Standards Associations, 2015)

2.9.1 Encabezado de la trama del estándar IEEE802.15.4

Para poder realizar operaciones de seguridad se hacen necesarios unos campos definidos dentro de las tramas IEEE 802.15.4. En la figura 5 se presenta la cabecera de la capa MAC del estándar IEEE802.15.4.

-Frames de control

-Auxiliary Security header.

-Frame Payload

-FCS

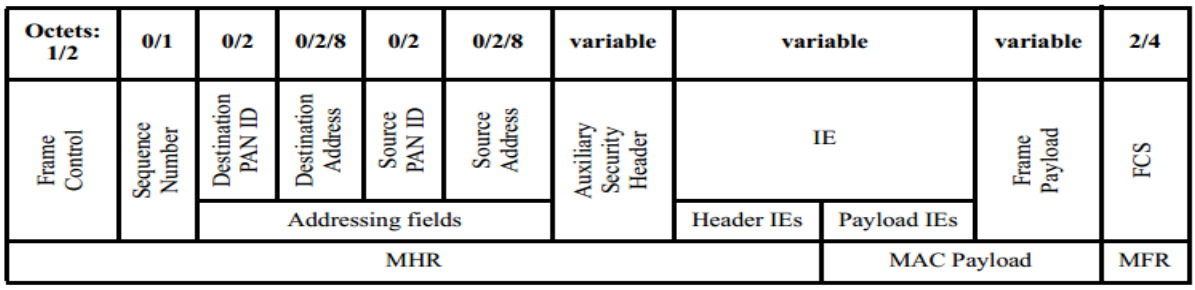


Figura 5. Cabecera de la capa MAC IEEE802.15.4. *(IEEE Standards Associations, 2015)*

La opción *auxiliary security header* solo se puede activar si el bit *security enable* del *frame* de control se encuentra en la opción 1.

La cabecera *auxiliary security header* será presentada en la figura 6.

Octets: 1	0/4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Figura 6. Formato de auxiliary security header. *(IEEE Standards Associations, 2015)*

-Security Control: Este parámetro presenta la información de seguridad que es aplicado a esta trama. En la figura 7 se puede apreciar el formato del campo de seguridad de control.

Bit: 0–2	3–4	5	6	6–7
Security Level	Key Identifier Mode	Frame Counter Suppression	ASN in Nonce	Reserved

Figura 7. Formato del campo de seguridad de control. *(IEEE Standards Associations, 2015)*

Los subcampos descritos en *security control* son el lugar donde se encuentra descrita la política de seguridad que selecciona el modo de funcionamiento de AES y el modo de identificación que se utiliza para la clave, el cual puede estar descrito implícitamente o explícitamente.

El subcampo *Security Control* es el lugar donde se ubica la política de seguridad, que seleccionará el modo de funcionamiento del cifrado de AES y el modo de identificación de la clave, que puede ser implícito o explícito. El resto del espacio está reservado para posibles ampliaciones. Los valores descritos para *key identifier mode* son:

- Cero (0) cuando el valor de la clave es conocida de manera implícita tanto para el emisor como para el receptor, por lo cual no se encuentra especificado dentro del mensaje.

-Uno (1) cuando la clave de identificación se encuentra de manera explícita con el byte definido por el *key Index* y el parámetro estático *macDefaultKeystore*, la identificación de la clave se realiza con el byte de *key index* y los 4bytes del *key source*.

-Dos (2) la identificación de la clave se realiza de manera explícita con el byte de *key index* y los 8 bytes de *key source*. (IEEE Standards Associations, 2015) (Carlos Garcia Arano, 2010)

La seguridad que se le realiza a cada una de las tramas, la debe realizar el receptor en cada una de las tramas recibidas donde tiene que seleccionar la clave que le corresponde, seguidamente actualiza los valores del contador con la respectiva operación criptográfica correspondiente. Esto permite que el nodo envíe tramas con diferentes niveles de seguridad.

-Frame Counter: Es un contador proporcionado por el emisor de la trama la cual permite proteger ante diversos ataques de repetición, por lo tanto cada mensaje provee un número de secuencia único el cual se encuentra representado por este campo. En las primeras versiones del estándar los *frames* cuentan con un único contador para los *frames* de salida, en la última versión del estándar se permiten múltiples contadores cada uno de los cuales está asociado a una clave. (IEEE Standards Associations, 2015)

-Key Identifier: Es un campo de longitud variable que identifica las claves usadas en la protección cifrada de los *frames* de salida. Dentro de este campo también se presenta la

información del originador de la clave de grupo y provee una identificación única para las diferentes claves que pueda tener un mismo originador. (IEEE Standards Associations, 2015)

2.9.2 Campo security Level.

El campo *security level* indica la actual protección del *frame*. Este valor puede ser adaptado sobre la base de *frame* por *frame* permitiendo realizar cambios en niveles de autenticación y la confidencialidad de los datos. Este campo define los diferentes niveles en que puede funcionar el algoritmo AES para proporcionar autenticación e integridad. Tiene 3 bits para seleccionar el nivel de seguridad, en el primero no realiza ningún tipo de operación criptográfica. (IEEE Standards Associations, 2015)

Los 3 bits de este campo permiten seleccionar entre 8 niveles de seguridad, desde lo más bajo, que no realiza ninguna operación criptográfica, hasta el nivel que ofrece más garantías. En tabla 1 se presenta cada uno de los niveles de seguridad que ofrece el estándar IEEE802.15.4. (IEEE Standards Associations, 2015)

Tabla 1 Niveles de seguridad disponible en la subcapa MAC

Security level	Security level field b2 b1 b0	Security attributes	Data confidentiality	Data authenticity	MIC length (octets)
0	000	None	OFF	NO	0
1	001	MIC-32	OFF	YES	4
2	010	MIC-64	OFF	YES	8
3	011	MIC-128	OFF	YES	16
4	100	Reserved			
5	101	ENC-MIC-32	ON	YES	4
6	110	ENC-MIC-64	ON	YES	8
7	111	ENC-MIC-128	ON	YES	16

Extraída de IEEE Standards Associations, 2015,pp. 373

La sigla MIC hace referencia a *message integrity code.*

2.10 Advanced Encryption standard (AES)

Es un estándar para cifrar adoptado por el gobierno de EEUU, el cual surgió como una sustitución para las vulnerabilidades de *Data encryption Standar* (DES). AES se considera

como uno de los algoritmos de cifrado simétrico más populares dado su robustez frente a herramientas de criptoanálisis. Dentro de la política de la National security agency describe que puede utilizarse para información *top secret*.

Una de las características de la criptografía requiere que los interlocutores puedan compartir la clave de cifrado de forma segura. Uno de los aspectos más importantes en los algoritmos de criptografía de clave simétrica es el tamaño de las claves. A continuación se describen algunas recomendaciones otorgadas por la *National institute of standards and technology* (NIST) para la generación de las claves. (NIST, 1996)

- Las claves deben ser generadas de forma aleatoria para reducir la probabilidad de que un atacante las pueda deducir o que estas puedan ser reutilizadas.
- Las contraseñas deben ser cambiadas de forma frecuente para disminuir la posibilidad que sean descubiertas utilizando técnicas de criptoanálisis.
- Las claves deben ser protegidas cuando van a ser almacenadas, de esta forma se garantiza que las comunicaciones no puedan ser descifradas.
- Las contraseñas deben ser protegidas durante su transmisión.
- Cuando las contraseñas no se utilicen deben ser eliminadas.

La criptografía secreta tiene ciertas limitaciones cuando se incrementan el número de nodos dentro de la red debido a que si se quiere establecer la comunicación cada nodo debe almacenar una clave, lo que involucraría que se hicieran necesarias $\frac{n(n-1)}{2}$ claves para poder comunicar n nodos entre se garantiza la integridad de cada una de las conexiones punto a punto. Cuando se utiliza el algoritmo de AES el cifrador se considera como una caja negra que necesita dos entradas: un bloque de tamaño fijo y una clave que debe tener el mismo tamaño. Con los datos obtenidos se debe obtener un bloque del mismo tamaño. El algoritmo de AES tiene la característica de que si el mensaje no es múltiplo de 128 bits, el último bloque debe rellenarse antes de pasar al cifrador. Este relleno no genera inconvenientes cuando se utiliza CTR que usa una XOR eliminando los bits que sobran.

Cuando el número de mensaje es mayor que uno el estándar IEEE802.15.4 define tres mecanismos:

AES-CBC-Mac que permite la autenticación y la integridad. El *message integrity code* es agregado al final de los datos. Su longitud depende del nivel de seguridad especificado en el campo *security policy*. La *message integrity code* es creada a partir del cifrado de la cabecera MAC y el *payload*. (Libelium, 2016)

AES-CTR para la confidencialidad. Todos los datos son cifrados con una clave de 128bits con algoritmo de AES, el contador de *frame* coloca un único *message ID* y el *key counter* es utilizado por la capa de aplicación si el contador de *frame* llega a su valor máximo. (Libelium, 2016)

AES-CCM para la confidencialidad y la autenticación. Este modo combina los dos métodos AES-CBC-MAC y AES-CTR. (Libelium, 2016)

2.11 AES-CBC de la capa MAC.

Este modo se utiliza para autenticar los mensajes. En esta parte cada bloque toma como entradas el resultado de su anterior y el bloque del mensaje correspondiente para generar un bloque del mismo tamaño con la información cifrada. El primer bloque se inicia con cero. Con esto se obtiene resumen o hash de 128 bits los cuales son obtenidos a partir del mensaje y la clave. Este mensaje es utilizado para anexarlo al mensaje que se desea enviar. Esto le permite al receptor comprobar la veracidad del mensaje realizando el mismo procedimiento del nodo transmisor y lo compara con el resumen anexado, si este concuerda se puede decir que el nodo transmisor conoce la clave de cifrado y que este mensaje no ha sido modificado o alterado.

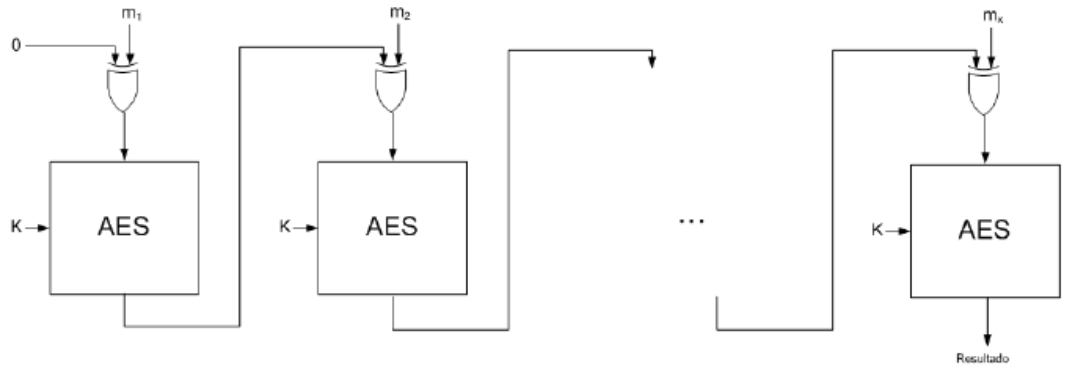


Figura 8. AES-CBC-MAC *(Carlos Garcia Arano, 2010)*

El estándar IEEE802.15.4 describe que de los 128 bits que son generados, se les pueden anexar los bits en su totalidad o únicamente 64 o 32 bits que son los menos significativos. A medida que el tamaño del paquete sea mayor, un atacante puede tratar de buscar la clave utilizando la fuerza bruta si la clave sigue siendo la misma. Como ejemplo un intruso puede

utilizar 2^{64} códigos MIC para autenticar un mensaje CBC-MAC64. (Carlos Garcia Arano, 2010)

2.12. Orientación de los mecanismos de seguridad.

Las principales amenazas en las redes de sensores inalámbricos van direccionadas a explotar las características del canal de comunicación inalámbrico y las condiciones del entorno físico donde se deben situar estos nodos.

Los mecanismos de seguridad que se orienten a las redes de sensores inalámbricos realicen deben estar orientados a los siguientes aspectos.

- Garantizar la confidencialidad debido a las características del canal de comunicación. (Carlos Garcia Arano, 2010)

- Autenticación de los datos transmitidos por los nodos debido al uso de un canal de comunicación no guiado. (Carlos Garcia Arano, 2010)

- Garantizar la integridad de la información evitando cualquier tipo de modificación que se pueda dar de forma accidental y de forma mal intencionada. (Carlos Garcia Arano, 2010)

- Garantizar la disponibilidad de los nodos y el canal de radio evitando que se origine una denegación de servicio. (Carlos Garcia Arano, 2010)

- Garantizar la accesibilidad lógica para los diferentes nodos aceptados dentro de la red. (Carlos Garcia Arano, 2010)

- Garantizar que no exista suplantación de nodos o que existan intrusos que accedan a la red, los cuales puedan inyectar datos maliciosos que afecten a la red con información falsa. (Carlos Garcia Arano, 2010)

2.12.1 Seguridad en redes de sensores inalámbricos.

A continuación se van a describir los diferentes ataques presentes a la red de sensores inalámbricos.

- El primero de estos es el ataque por denegación de servicio DoS. Este ataque se genera desde el nivel físico cuando el nodo intruso inunda el canal de comunicación con datos para consumir el ancho de banda presente en la red. (Suescún, 2009)

- La colocación de nodos corruptos que buscan suplantar los nodos en la red esto lo realizan ya sea por software o hardware.

    - Recolectando información o *sniffer* en la red. Lo que se busca es que el nodo intruso capture o recolecte la información que pasa a través de este, después con esta información se busca realizar un daño al sistema. (Suescún, 2009)

    - Ataques físicos sobre los nodos en el cual estos son extraídos de la red generando inconvenientes dentro de esta y robándose la información de criptografía almacenada en ellos. (Suescún, 2009)

    - Otro tipo de ataque es el *SinkHole*, en el cual se coloca un nodo intruso cerca del nodo base para atraer información de tipo confidencial. (Suescún, 2009)

    - Existe otro tipo de ataque llamado *Sybil* donde el atacante coloca diferentes nodos con identidades no legales o que fueron hurtadas de la red. (Suescún, 2009)

Para mitigar los diferentes tipos de ataques las redes de sensores involucran el uso de esquemas de cifrado y esquemas de manejo de claves, con esto se evita que si algún tipo de intruso se llega a robar un nodo no pueda realizar una captura de todas las claves de la red.

Cuando las redes son homogéneas se manejan piscinas de claves. Una de sus principales limitantes presentes es que necesitan que los nodos tengan gran cantidad en el almacenamiento. Para las redes heterogéneas existen nodos tipo *cluster*, esto incluye nodos superiores y lo que se busca es que la comunicación entre los nodos se establezca a partir de la comunicación con los superiores.

2.12.3 Tipos de ataque.

Los tipos de ataque se analizarán de acuerdo a cada una de las capas del modelo TCP/IP, la capa de red, transporte y aplicación. Su funcionamiento es descrito por Zigbee y las dos capas

inferiores son definidas por el estándar IEEE802.15.4. A continuación Figura 9 se presenta el modelo de capas TCP/IP ajustado. (Carlos Garcia Arano, 2010)

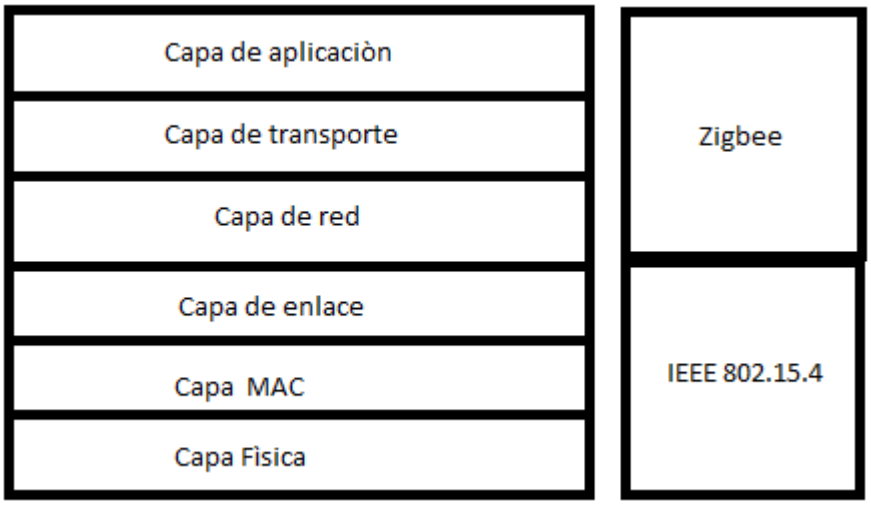


Figura 9. Modelo de capas nodo sensor IEEE802.15.4

Los ataques pueden ser descritos de acuerdo donde se ubique el atacante con respecto a la red. Si la amenaza no se ubica dentro de la red se considera *outsider* y sus ataques verán limitada su capacidad de hacer daño y si el ataque se ubica dentro de la red el tipo de daño que puede generar tiene el potencial de tener un mayor impacto.

2.12.3.1 Ataques a la capa física IEEE802.15.4.

Esta vulnerabilidad es atribuible a la dificultad de asegurar el espacio físico de los nodos, debido a que en algunas de las aplicaciones los nodos son desplegados en zonas rurales donde se dificulta tener mecanismos eficaces para el mantenimiento o la salvaguarda de los nodos. Esto genera que algún intruso que tenga acceso a los nodos sea capaz de generar un daño físico al nodo o extraer información que tenga almacenado este. Algunos nodos en su arquitectura hardware, poseen características para evitar la lectura/escritura sobre la memoria. (Carlos Garcia Arano, 2010)

La otra vulnerabilidad presente en la capa física se atribuye a las interferencias presentes en el canal de comunicación, la cual puede provenir de diferentes fuentes, ya sea por dispositivos Wi-Fi, bluetooth o maquinaria industrial. Estas fuentes pueden ser intencionales (*jamming*) o accidentales. Este tipo de interferencias puede bloquear la comunicación entre los nodos de forma permanente ocupando el canal de comunicación, también puede de forma reactiva escuchar el canal de comunicación y generar colisiones cuando perciba que algunos de los nodos se están comunicando. Esto contribuye a que existan restricciones a la disponibilidad

de la red. Para este tipo de vulnerabilidad se definen métodos de autenticación para identificar algún nodo intruso que quiera ocupar el canal de comunicación. Otro aspecto para mitigar este tipo de interferencia se encuentra inmerso en el estándar. Este utiliza como modulación la técnica de espectro ensanchado de secuencia directa, el cual ofrece alta resistencia a la interferencia y como mecanismo de acceso utiliza sensado de portadora evitando colisiones y el tiempo de acceso garantizado. Con esto se busca evitar las colisiones dentro del canal de comunicación, además tiene un mecanismo de CCA (*Clear Channel Assess*) para evaluar el canal antes de transmitir. (Carlos Garcia Arano, 2010) (Suescún, 2009)

2.12.3.2 Ataques a la capa MAC IEEE802.15.4

Los ataques en esta capa son más sofisticados por sus patrones de ataque. Un ejemplo de esta es *sleep deprivation torture*, la cual es una vulnerabilidad que genera colisiones intencionadas de forma continua para generar retransmisiones de las tramas de datos evitando que el nodo pase a modo de espera. En este ataque se utilizan técnicas como *jamming*, inyección de tramas NAK. (Carlos Garcia Arano, 2010)

Existen otras técnicas que están enfocadas al uso de *beacons* cuyas tramas son legítimas utilizadas como ataques de repetición. Dentro del estándar se describen características de etiquetado en la numeración de los paquetes para contrarrestar este tipo de ataques.

Otra técnica es el ataque *Sybil* donde el nodo malicioso presenta diversas identidades dentro de la red, invalida la información de los legítimos y modifica la información de enrutamiento. Para confrontar este ataque han propuesto una metodología de protección mutua entre los nodos y el conteo de las tramas que son transmitidas por cada nodo. En la figura 10 se presenta un ataque tipo *Sybil*. (Suescún, 2009) (Carlos Garcia Arano, 2010)

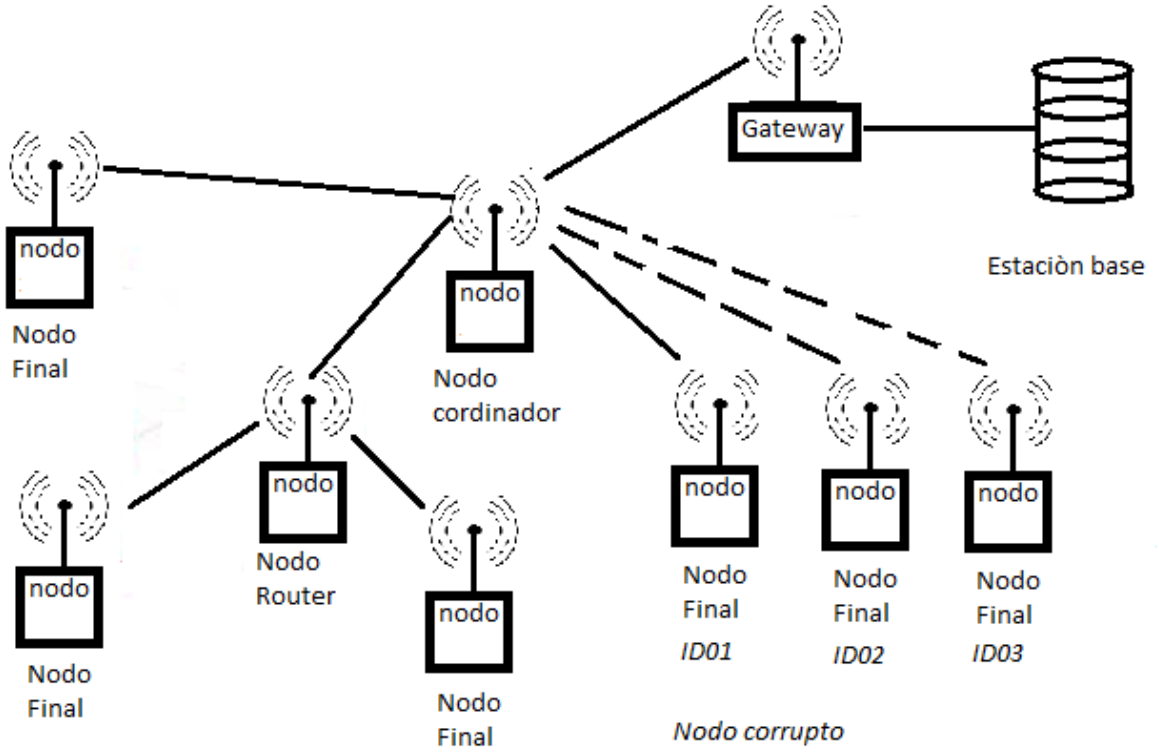


Figura 10. Ataque de Sybil nodo intruso

2.12.3.1. Ataques a la capa de red Zigbee.

Este ataque es realizado por nodos que se encuentran dentro de la red, los cuales funcionan como enrutadores FDD sin ser coordinadores. Afectan a los algoritmos de enrutamiento de la red inyectando dentro de la red información falsa, lo cual genera que no se tenga disponibilidad en la red. El comportamiento que se genera es llamado *Sinkhole.* El nodo que está comprometido muestra rutas de buena calidad hacia diferentes partes de la red buscando que la información que pase a través de él se pierda, logrando convertirse en un sumidero para la información que es difícil de detectar. La detección de este tipo de nodos es compleja, por ende se busca garantizar que los nodos que hacen parte de la red se encuentren autenticados. Sin embargo se presentan variaciones con niveles de falsificación más complejos donde se utilizan enlaces con baja latencia para falsificar las distancias presentes entre los nodos y de esta forma generando un túnel para la información. Estos nodos pueden operar como "*relays*" pueden modificar las condiciones de enrutamiento incluyendo algunas veces técnicas de criptografía y autenticación. Para mitigar un poco este tipo de ataque se incluyen algoritmos que tienen en cuenta la posición geográfica de los nodos para realizar el enrutamiento de los datos. A continuación en la figura 11 se presenta un ejemplo de este tipo de ataque. (Carlos Garcia Arano, 2010) (Suescún, 2009)

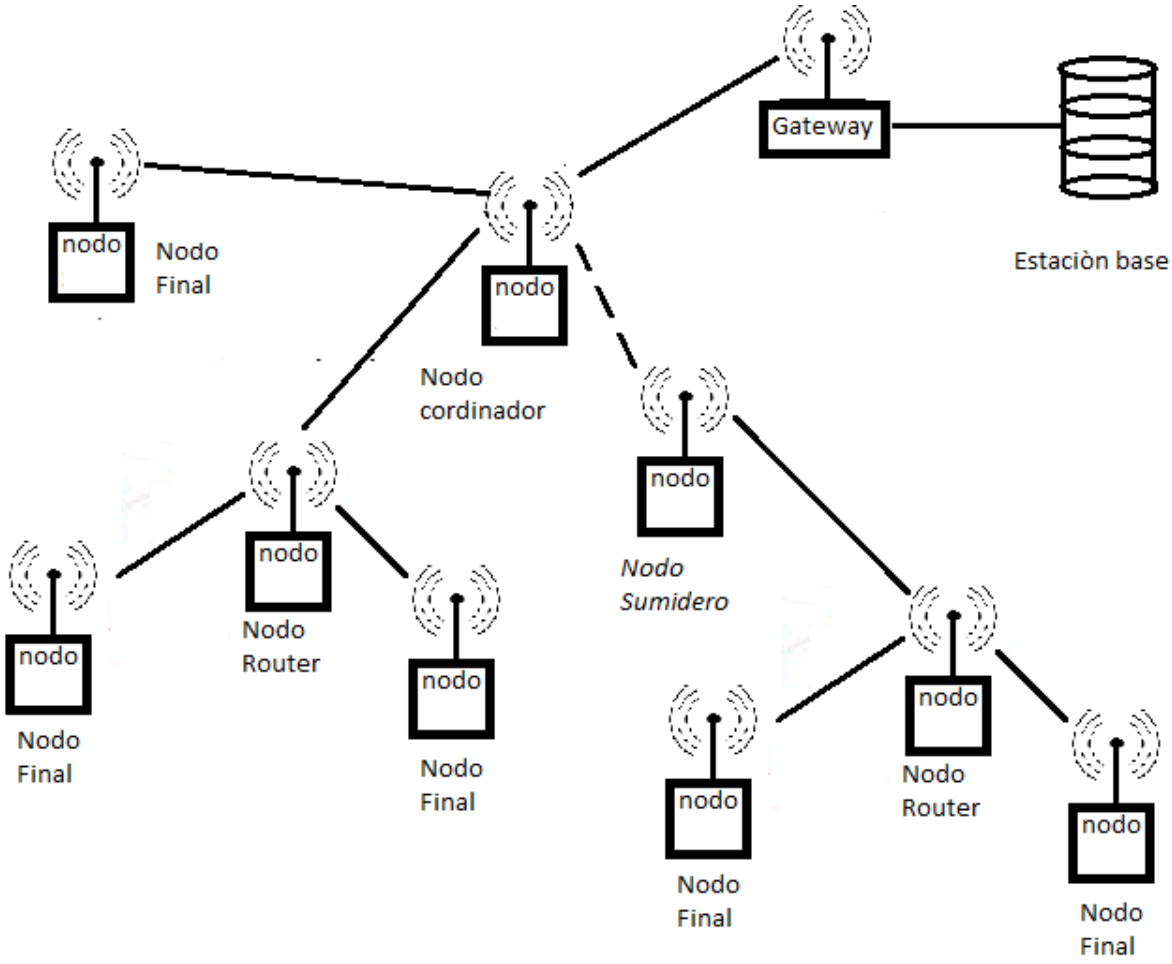


Figura 11. Ataque nodo sumidero.

Existe otro tipo de ataque llamado *Hello Food* donde el nodo intruso se le conecta una antena de alta ganancia para confundir a los nodos que hacen parte de la red, dado que se presenta como un nodo vecino de un gran número de sensores. Sin embargo estos no tienen la suficiente potencia y ganancia de la antena para comunicarse con este nodo. Con esto se busca que exista un acelerado consumo de las baterías. En la figura 12 se puede apreciar que un nodo tiene una antena de alta ganancia con la cual puede interrumpir las comunicaciones de los otros nodos de la red. (Carlos Garcia Arano, 2010) (Suescún, 2009)

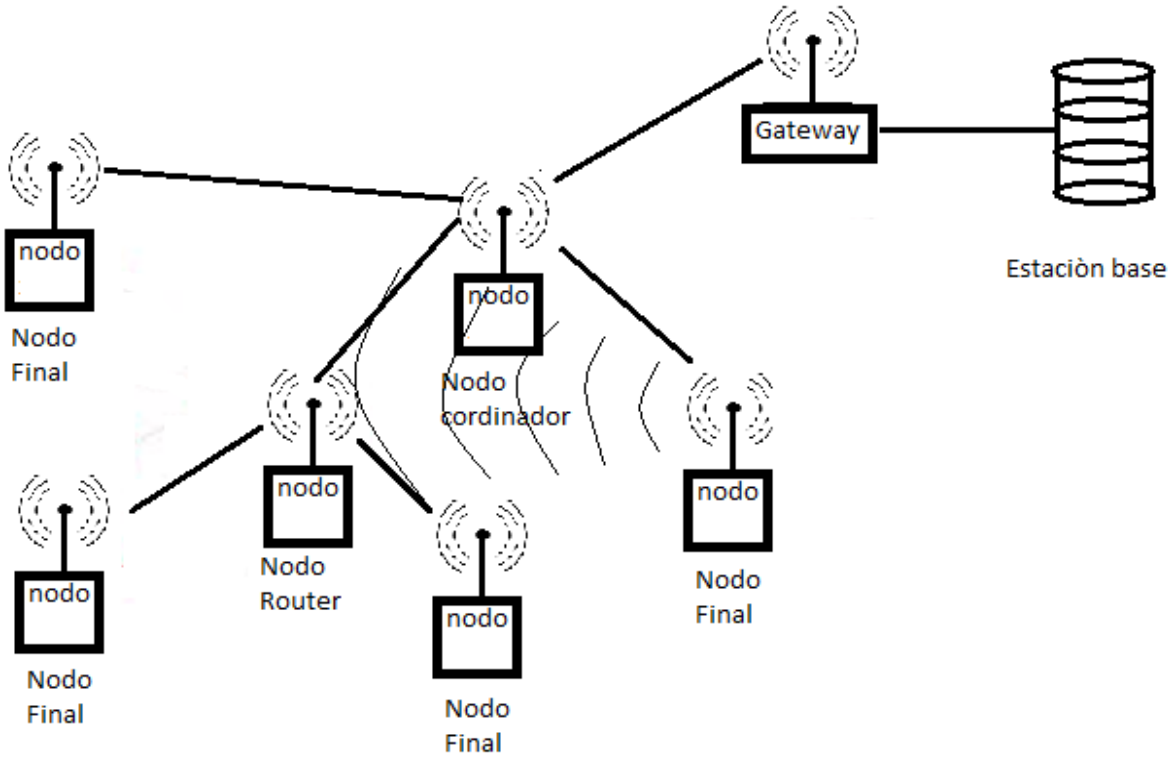


Figura 12. Nodo intruso con antena de alta ganancia.

2.12.3.4 Ataques en la capa de aplicación Zigbee.

Los ataques definidos para la capa de aplicación dependen del tipo hacia donde se está orientando el funcionamiento de los nodos que hacen parte de la red de sensores inalámbricos. Dependiendo del lenguaje de programación y de la forma de codificación se pueden encontrar múltiples vulnerabilidades tales como el desbordamiento de *buffer* y la inyección de parámetros. (Carlos Garcia Arano, 2010)

El estándar también provee mecanismos para garantizar la confidencialidad y autenticidad de la información transmitida. El estándar IEEE 802.15.4 soporta el uso de cifrado AES (*Advanced Encryption Standard*) de los paquetes salientes. La autenticación de los datos se puede comprobar incluyendo un código de integridad de mensaje (MIC) en cada *frame*. (Jimena Garbarino, 2011)

2.13 Estado del arte para la seguridad en redes de sensores.

La seguridad en redes de sensores tiene gran importancia por la diversidad de aplicaciones encontradas en diversos ámbitos como son la agroindustria, domótica, vehículos autónomos, fuerzas militares o salud, entre otros.

Uno de los primeros trabajos sobre la seguridad en redes de sensores inalámbricos se encuentra en el desarrollo de protocolos seguros para las redes de sensores inalámbricos. (Adrian Perrig, 2001). SPINS define dos bloques de seguridad que buscan definir las primitivas de confidencialidad, autenticación e la integridad de los datos es decir que no han sido modificados. Con este protocolo se resuelve de forma eficiente la autenticación en *broadcast* de los sensores, utilizando las características de hardware mínimo que tienen estos dispositivos.

Uno de los principales aportes presentados en este trabajo es el desarrollo del protocolo TESLA (*Time, efficient,streaming, Loss-tolerant Authentication protocol*), el cual le provee autenticación al *streaming* realizado en *broadcast*. Además presenta el diseño e implementación del protocolo SNEP (*Secure Network Encryption protocol*), el cual provee confidencialidad, datos recientes y que estos no hubieran sido reemplazados por anteriores mensajes, con poca carga en las cabeceras. También presenta mecanismos de autenticación en cuanto a los protocolos de enrutamiento. Los nodos utilizados para la implementación de estos protocolos utilizan el sistema operativo tinyOS.

Otro de los principales aportes se dieron en cuanto al análisis de seguridad en redes de sensores, el cual fue descrito por (Madhukar Anand, 2006). Allí se expone que las redes de sensores no se pueden considerar como dispositivos de cómputo tradicionales donde los métodos y modelos de seguridad se consideran suficientes. A las redes de sensores inalámbricos se le deben incluir nuevas características para soportar los mecanismos de seguridad. Los nuevos mecanismos de seguridad deben considerar que un atacante puede capturar físicamente los nodos y leer sus llaves secretas, además puede interceptar o inyectar nuevos mensajes. La jerarquía en la naturaleza de las redes y el mantenimiento de las rutas le permiten a un atacante determinar la ubicación del nodo. Otro aspecto importante es que las redes de sensores dependen de la redundancia para la captura de información de un entorno de forma precisa, esto implica el despliegue de varios nodos en la red.

Dentro de este trabajo se expresan tres categorías de ataque las cuales se relacionan a continuación.

Espionaje: El adversario determina qué tipo de datos están a la salida de las redes de sensores escuchando los mensajes transmitidos por los nodos. Este tipo de ataque puede ser pasivo, donde el nodo atacante de forma pasiva escucha los mensajes. En el modo activo el nodo intruso envía peticiones a los nodos o busca agregar más nodos buscando ganar más información. La ubicación del intruso dentro de la red determina la cantidad de información que puede obtener.

Interrupción: El adversario interrumpe la aplicación del sensor. Este intruso debe atacar contra las locaciones de la red del sensor, lo cual puede influenciar de forma significativa en la salida de la red. Esto puede inducir a una interrupción semántica inyectando mensajes, datos corruptos o cambiando los valores de tal forma que se pueda agregar a la red. Esto se puede lograr modificando las condiciones del entorno del sensor un ejemplo de esto sería cambiando las condiciones de calor.

Secuestro: El atacante sabotea la aplicación de la salida del sensor ganando control sobre otros sensores. Este ataque selecciona el grupo de sensores permitiendo ataques de escucha e interrupción, los cuales se pueden realizar desde la parte interna de la red.

Seguidamente se encontraron trabajos enfocados a la descripción de las posibles vulnerabilidades presentes en las redes de sensores inalámbricos tal como lo presenta (Suescún, 2009). Dentro de este artículo se describen diferentes tipos de ataques los cuales son descritos a continuación.

Ataques de denegación de servicio: Donde los nodos atacantes envían gran cantidad de mensajes buscando consumir el ancho de banda, de esta forma se consigue la indisponibilidad temporal del nodo.

Nodos suplantados: Este ataque consiste en lograr incluir un nodo intruso en las redes de sensores, ya sea cambiando la dirección física o lógica del dispositivo, el cual inyecta información corrupta dentro de la red.

Nodos intrusos: Donde el nodo atacante escucha y recolecta la información de la red, de forma pasiva.

Ataques físicos: Donde el nodo se extrae de la red de forma física para extraerle información y capturar las contraseñas.

Ataque *sinkhole*: Este ataque consiste en colocar un nodo intruso cerca del concentrador de tal forma que pueda atraer información muy confiable.

Ataque *sybil*: En este el atacante introduce múltiples nodos con identidades que pueden ser hurtadas o ilegales.

Ataque de forma gusano: Las redes de sensores involucran como mecanismos de seguridad procesos de cifrado utilizando piscina de claves, este esquema debe realizarse de tal forma que si algún intruso accede captura el nodo no pueda capturar la clave de la red.

También surgieron trabajos de investigación enfocados a analizar los mecanismos de seguridad que presenta el estándar IEEE802.15.4 (Carlos Garcia Arano, 2010). Dentro de este proyecto de investigación se realiza un análisis del impacto de las funcionalidades de seguridad que se encuentran presentes en el estándar IEEE802.15.4. Allí se describen los diferentes niveles de seguridad propuestos hacia el módulo hardware criptográfico. Además se desarrolló sobre la plataforma FreeRTOS para su capa MAC, el desarrollo propuesto dentro de este trabajo de master describe como estas funcionalidades pueden garantizar la integridad y confiabilidad de las comunicaciones. También se analiza el consumo del coste energético de este tipo de sensores los cuales se relacionan a los tiempos de consumo generados en la transmisión.

En los últimos años se han venido presentando trabajos de investigación enfocados al desarrollo de nuevos mecanismos de cifrado tal como lo describe (Martínez, 2015) .Dentro de este artículo se describe la seguridad de sensores inalámbricos basándose en funciones físicamente no clonables donde se encontró que entre los mecanismos para ofrecer seguridad en las redes de sensores inalámbricas se encuentra establecer claves entre los diferentes nodos de la red, la cual se encuentra almacenada en la memoria de cada uno de los sensores. Esta es una de las vulnerabilidades que se tienen como ataque físico para este tipo de dispositivos. Para evitar este tipo de ataques se presenta como salvaguarda la aplicación de funciones físicamente no clonables (PUFs) usados como primitivas criptográficas en conjunto con los módulos de descifrado y cifrado, lo cual permite proveer integridad, confiabilidad y autenticación en el nodo sensor. La implementación de un módulo de generación de llaves criptográficas dentro de los nodos basados en arreglos PUFs para establecer llaves seguras en el WSN.

Otro grupo de trabajos están siendo encaminados al modelado de ataques a las redes de sensores inalámbricos. A continuación se presentan los principales ataques a estos tipos de redes descritos en el trabajo (Alvaro Diaz Suárez, 2014).

Ataque *Jamming* el cual produce denegación de servicio a los usuarios autorizados con el envío de tráfico erróneo. Este tipo de ataques utilizan transmisión de señales de alta potencia

que colisionan con los paquetes verdaderos. Según el modo de introducir este tipo de señales las clasifica en ruido, tono, pulso, barrido y seguimiento.

Ataque *tampering*: En este caso tienen acceso físico al nodo para robarle la información interna del nodo.

Ataque *collision*: El nodo atacante no sigue el protocolo de control de acceso al medio generando colisiones. Una colisión se genera cuando dos nodos realizan transmisiones de forma simultánea sobre el mismo rango de frecuencias provocando que los paquetes lleguen corruptos.

Ataque *resourse exhaustion*: Dentro de este tipo de ataque se generan colisiones de forma repetitiva por las múltiples retrasmisiones del nodo que se esté atacando con esto se busca acabar los recursos de procesamiento y energía del nodo.

Ataque *energy drain*: Este tipo de ataque se aprovecha de las limitaciones en la alimentación del nodo. El ataque inicia con el envío de mensajes falsos en la red generando una cantidad de tráfico el cual es respondido por los nodos consumiendo sus recursos y respondiendo a las peticiones falsas en las cuales podrían eliminar nodos de la red.

Ataque *interrogation*: Este tipo de ataque explota el mecanismo *handshake* el cual es utilizado por diversos protocolos para evitar la pérdida de integridad de los mensajes. Esto se logra con el envío de mensajes *Require to send* para la obtención de respuestas *clear to send*.

Ataque *sniffing*: Esto sucede si los paquetes dentro de la red no viajan cifrados lo cual permite que estos sean leídos.

Ataque *black Hole*: Este tipo de ataque consiste en la alteración del enrutamiento de los paquetes en la red buscando atraer los paquetes hacia el nodo atacante el cual los va retirando del tráfico de la red.

Ataque *selective Forwards*: Este ataque se aprovecha de que en el caso de que no exista comunicación directa entre dos nodos se hace necesario enviar la información a través de nodos intermediarios lo cual podría ser aprovechado por un nodo atacante que se podría comportar como un nodo intermediario el cual podría eliminar o no propagar la información que le está llegando. Esta eliminación de los paquetes se puede hacer de forma aleatoria o eliminando paquetes específicos.

Ataque *Homing*: Para este tipo de ataque primero se estudia el tráfico de la red para identificar cuáles son los nodos considerados críticos como lo son los nodos coordinadores o los nodos circundantes al *gateway* para poder después deshabilitarlos.

Ataque *Sink Hole*: Dentro de este tipo de ataque busca atraer todo el tráfico cercano a un nodo intruso el cual genera una esfera de influencia atrayendo flujo de información que iba destinada hacia una estación base.

Ataque *hello Flood*: Este tipo de ataque lo que busca es consumir la energía de los nodos. Un atacante con un transmisor de alta potencia envía paquetes *HELLO* los cuales son contestados por varios nodos haciendo que estos gasten sus recursos energéticos.

Ataque *Misdirectio*n: Este tipo de ataque está enfocado en el envío de mensajes hacia un destino inalcanzable dentro de la red, esto obliga a que exista un consumo de potencia de los nodos por la cantidad de paquetes que debe procesar.

Ataque *node replication*: Este ataque consiste en que múltiples nodos intrusos se hacen pasar por un único nodo de la red.

Ataque *spoofing*: Este tipo de ataque consiste en la suplantación de un nodo de la red falsificando datos, busca alterar el enrutamiento para poder debilitar la red.

Ataque *flooding*: El atacante envía de forma continua solicitudes para nuevas conexiones buscando acabar los recursos de los nodos, de esta forma reduce su tiempo de vida.

Ataque *application*: Este ataque se concibe al realizar variaciones en el firmware del sistema embebido del nodo, para hacer esto generalmente el atacante debe tener acceso físico al nodo para realizar el proceso de programación.

Ataque *overwhelm*: Este tipo de ataque consiste en atacar de forma directa el sensor que se encuentra con el nodo de tal forma que la adquisición de señal adquirida sea errónea.

Este proyecto clasifica los ataques en pasivos y activos, los primeros de estos se consideran enfocados a la interceptación de las transmisiones para el robo de información y los activos buscan la inyección de información errónea, modificación de la información o suplantación de nodos.

3. Metodología.

3.1 Desarrollo de la red de sensores.

En esta etapa se presenta el diseño de la red de sensores que contempla la elaboración de una red tipo infraestructura donde se tiene un nodo coordinador y dos nodos finales configurados como router en uno de los nodos se contempla la medición de la variable temperatura.

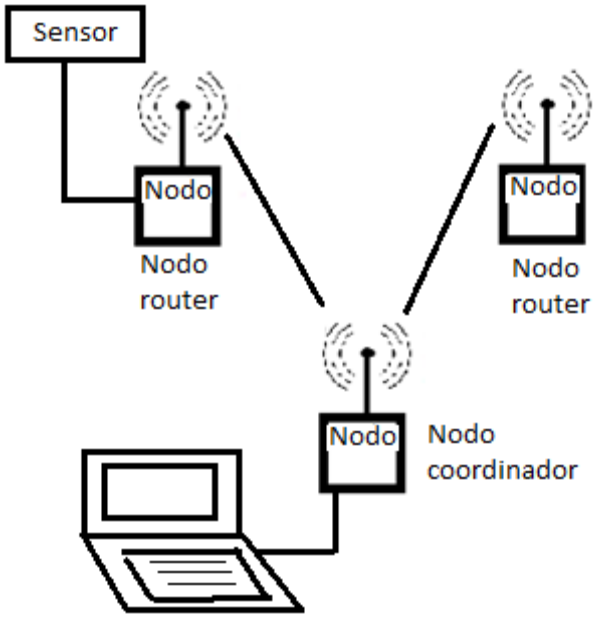


Figura 13 . Topología de red coordinador-router.

La información que es enviada hacia el coordinador es adquirida desde un aplicativo software desarrollado en javascript. Dicha información es cifrada para posteriormente ser transmitida por una conexión TLS hacia un servidor local o hacia un servidor remoto. Dentro de dicho servidor se almacena la información en una base de datos PostgreSQL.

Las tecnologías utilizadas para la construcción de las redes de sensores inalámbricos son diversas, las cuales difieren entre sus recursos hardware, el consumo de potencia, tamaño, costos, banda de frecuencias de operación y cobertura que proveen.

Para la elaboración de la red de sensores inalámbricos por capacidades hardware, firmware y accesibilidad se seleccionó el radio XBEE serie 2 del fabricante Digikey. Las principales características de este tipo de radio son:

- Son radios de bajo costo
- Interoperabilidad con el estándar IEEE802.15.4
- Son de bajo consumo de potencia para redes MESH.
- Interoperabilidad con radios de otros vendedores.
- Soporta largas y densas redes MESH
- 128-bit cifrado AES.
- Agilidad en frecuencia.

3.1 Desarrollo.

La red de sensores cuenta con un nodo coordinador y nodo router. El nodo coordinador está constituido por un radio xbee serie 2 del fabricante Digikey el cual está configurado en modo coordinador API con los respectivos parámetros para asociarlo al nodo router. Este nodo se conecta a una plataforma xbee-shield el cual tiene una interfaz USB que permite conectarlo al ordenador o Gateway. En la figura 14 se presenta el nodo coordinador utilizado.

Figura 14 . Nodo xbee cordinador

El nodo router puede funcionar como dispositivo final está constituido por un radio XBEE de la serie 2 configurado como nodo router AT y los respectivos parámetros para poderlo asociar al nodo coordinador. El firmware utilizado es ZB con función XB24-ZB, además se contempla para este nodo un circuito para la adecuación de señal para el sensor de temperatura LM35 y un sistema de alimentación que permite alimentar el nodo con batería o con un cargador de 9 voltios. En la figura 15 se presenta el plano electrónico y en la figura 16 se presenta el prototipo con el nodo router.

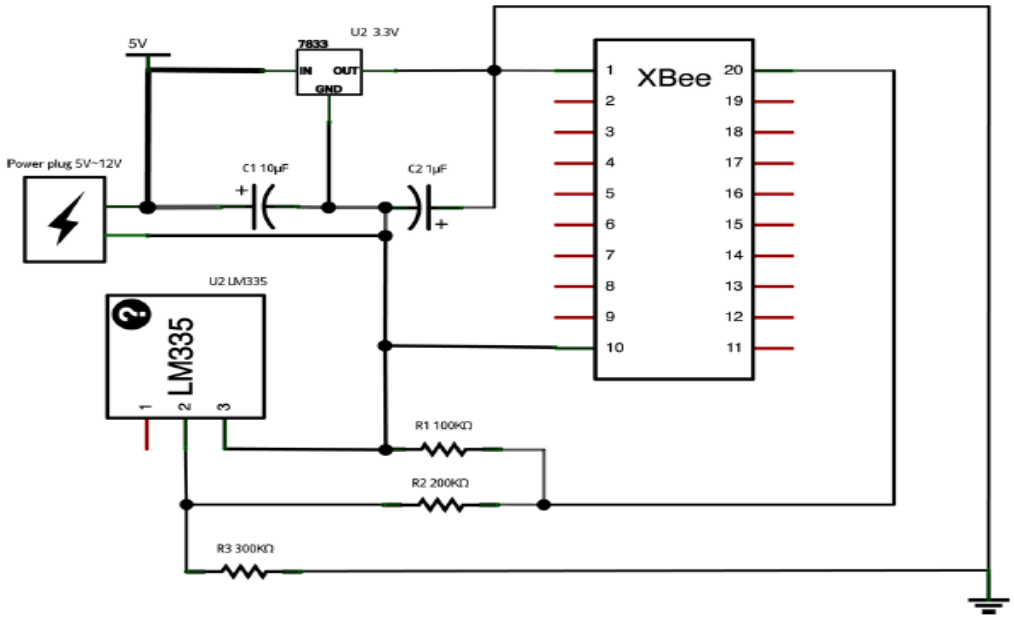


Figura 15, Plano electrónico del nodo router para medir temperatura. *(Faludi, 2010)*

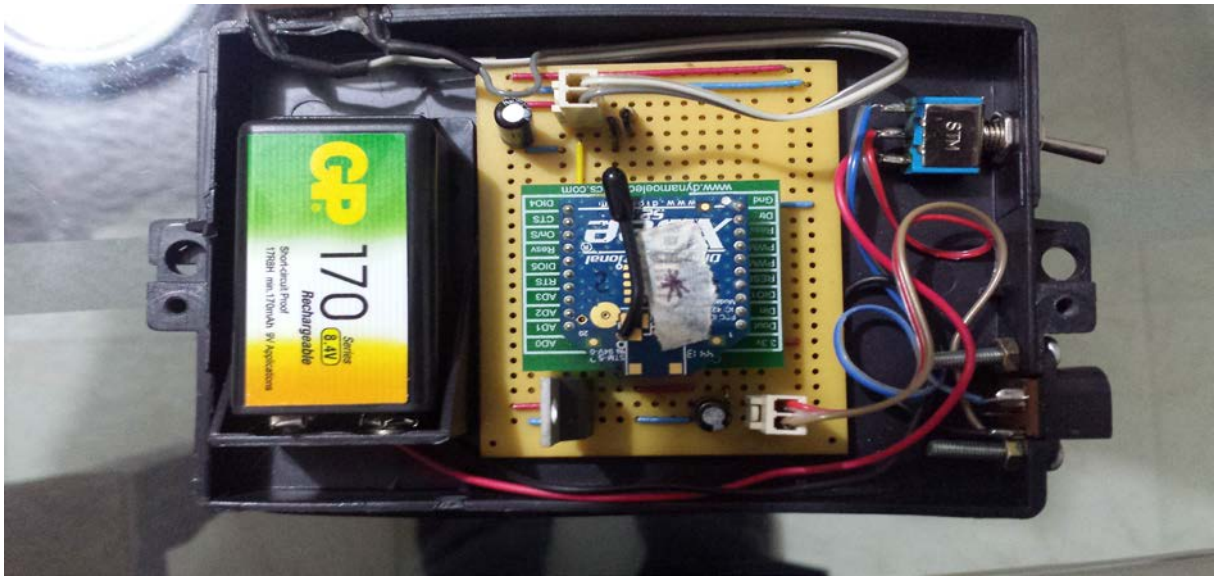


Figura 16. Nodo XBEE para el monitoreo de temperatura elaborado.

3.1.1 Seguridad en los nodos de comunicación XBEE

Cuando se habilita la seguridad en los nodos XBEE Zigbee, estos adquieren una llave de red. Esta llave se activa a partir de un código semilla de tal esta forma la transmisión de los datos son cifrados con esta llave.

Para activar la seguridad de estos nodos sobre el dispositivo, ha de habilitarse la opción *encryption enable* (EE). Este parámetro debe ser colocado en uno y cuando se configura el

módulo XBEE, ya no se identificará con los otros nodos de la red utilizando el PAN ID y el canal en el cual estaba operando, todas las transmisiones en este modo van a estar cifradas.

El módulo XBEE coordinador define dos formas para establecer la seguridad. La primera de estas involucra la inclusión de una clave que permite la creación de la clave de cifrado de red, si no se define esta clave se generará una clave aleatoria la cual genera la llave para el cifrado de la red. La clave de red es administrada por el nodo coordinador a los nodos router y los nodos finales, esta clave puede ser compartida por una configuración cifrada.

3.1.2 Configuración de los nodos XBEE.

Para la configuración de los radios XBEE se utilizó el software libre X-CTU el cual es una herramienta software multiplataforma que permite interactuar con los dispositivos digikey. En la figura 17 se presenta la configuración del nodo utilizando el X-CTU.

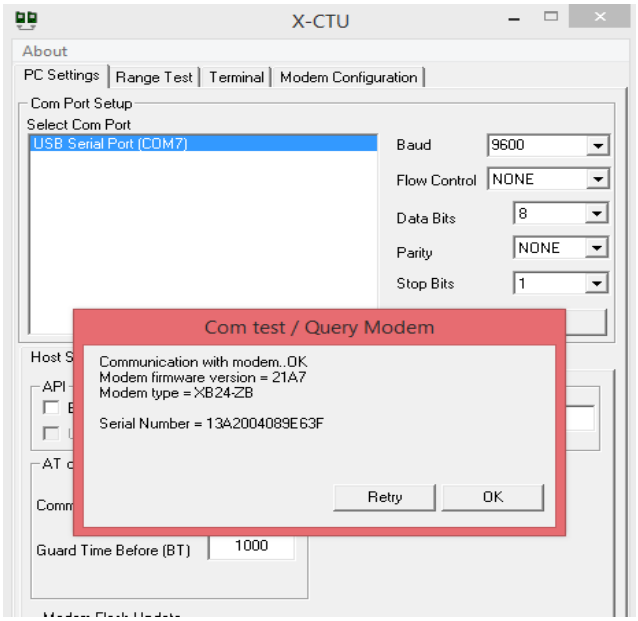


Figura 17. Configuración de los nodos XBEE con X-CTU

Dentro de los parámetros de configuración al nodo router se le configuró su módulo de conversión análogo digital con una frecuencia de muestreo de 1 segundo.

En la figura 18 se presenta la configuración de seguridad en el nodo XBEE como coordinador.

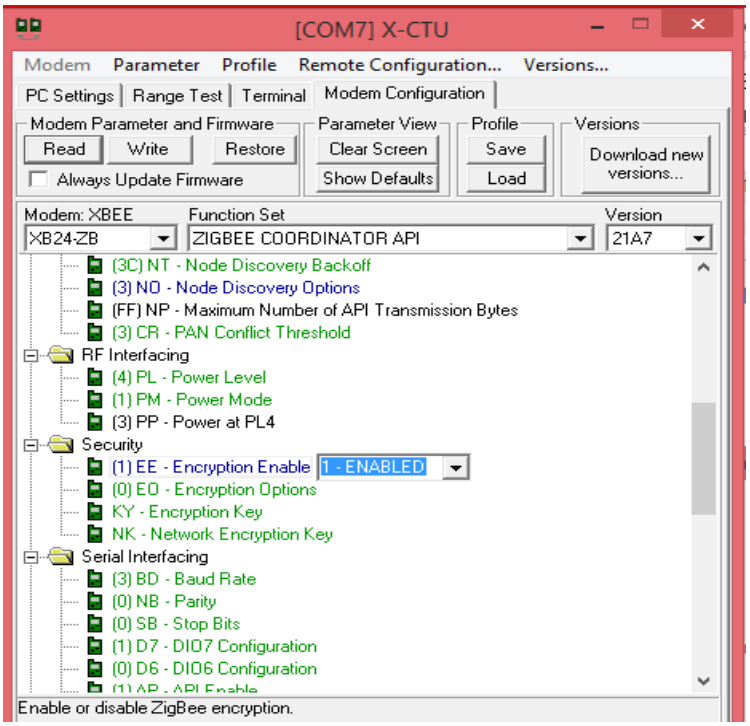


Figura 18. Cifrado del nodo XBEE con el x-ctu

Seguidamente se asignó la clave de cifrado en formato Hexadecimal. En la figura 19 se presenta la configuración de este campo.

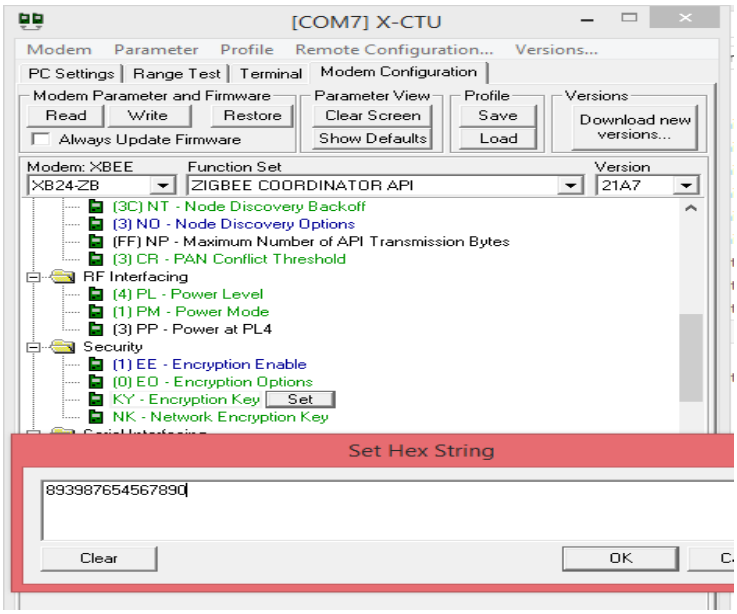


Figura 19. Asignación de clave para cifrar los datos.

Para la validación del cifrado de los paquetes se realizó la adquisición del radio 1322x USB *dongle* del fabricante freescale el cual cuenta con el módulo MC1322x LGA *platform –in-package* (PIP). Este dispositivo puede ser utilizado en aplicaciones inalámbricas punto a

punto y en redes *mesh* basadas en *Zigbee*. Este radio tiene compatibilidad con el estándar IEEE802.15. 4 y *Zigbee*. (Free Scale, 2010) Para el caso de este proyecto se utiliza este radio en modo *sniffer* el cual permite la captura de los paquetes que utilizan el estándar IEEE802.15.4 esto permite evaluar el algoritmo de cifrado configurado en los radios XBEE. En la figura 20 se presenta el dispositivo 1322x USB utilizado.

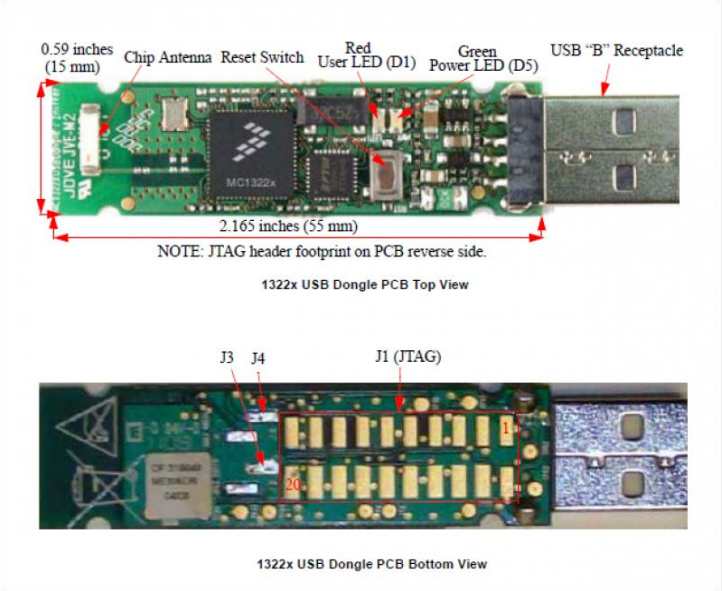


Figura 20. Nodo base MC1322x compatibilidad con el IEEE802.15.4 Sniffer *(Free Scale, 2010)*

Para realizar el proceso de *sniffer* se utilizó el software WiresharkZigbeeUtility el cual permite realizar la canalización de la captura que realiza el *dongle* MC1322x con el software wireshark. (jbthomsen, 2016)

Para el funcionamiento de este modo se debe definir el canal en el cual se están realizando las transmisiones en este caso es el canal 14 el cual fue configurado previamente en los nodos y el puerto del módulo es el puerto número ocho. En la figura 21 se presenta la configuración del *wireshark zigbee Sniffer pipe wrapper.*

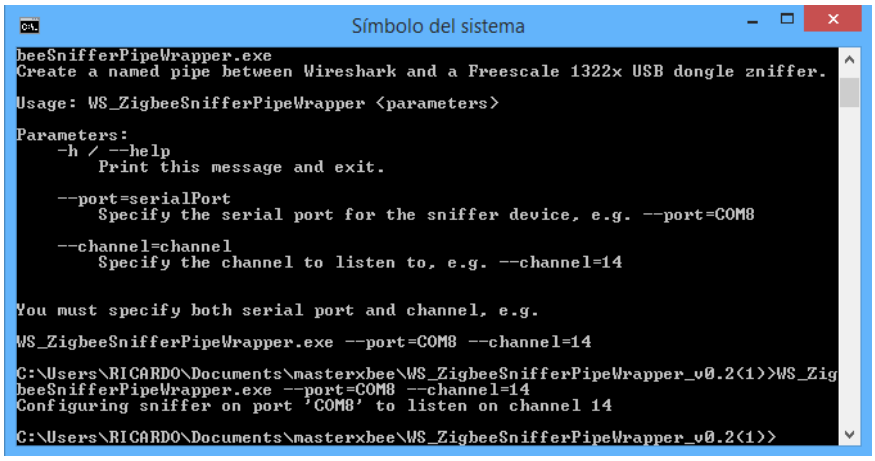


Figura 21. Configuración del sniffer

Seguidamente se realizó la ejecución del aplicativo software *wireshark* donde se selecciona como interfaz el ws_ZigbeeSnifferPipeWrapper para realizar la captura de los paquetes. En la figura 22 se presentan las capturas de los paquetes Zigbee utilizando la herramienta *wireshark* utilizando como interfaz hardware el dongle MC1322x.

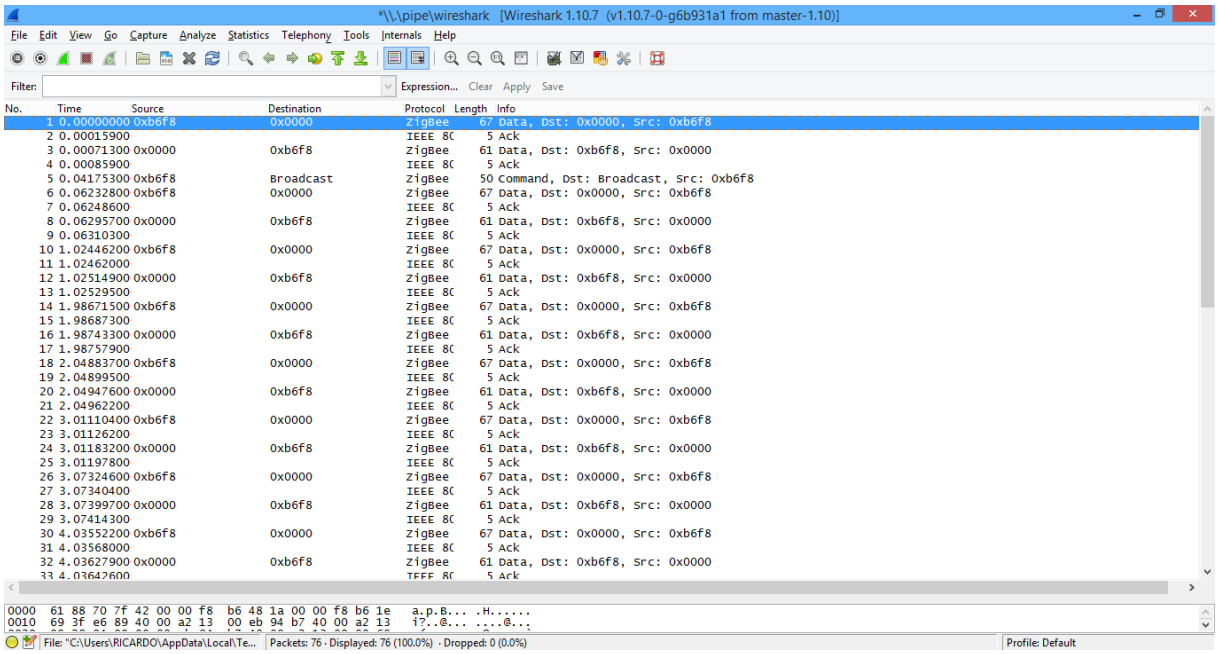


Figura 22. Captura de los paquetes Zigbee con wireshark.

Después se analizan cada uno de los paquetes capturados por *wireshark*. Al analizar los paquetes utilizando se pudo validar que los datos se encuentran cifrados y los paquetes tienen añadido un MIC. Con esto se garantizará la confiabilidad e integridad de los datos que se están transmitiendo. El campo *security field* en sus tres primeros bits están configurados con

111 lo cual está representado por el número 28. En la figura 23 se presenta el campo *security control field* con su valor resaltado en *AZUL, el Message Integrity code y los datos cifrados.*

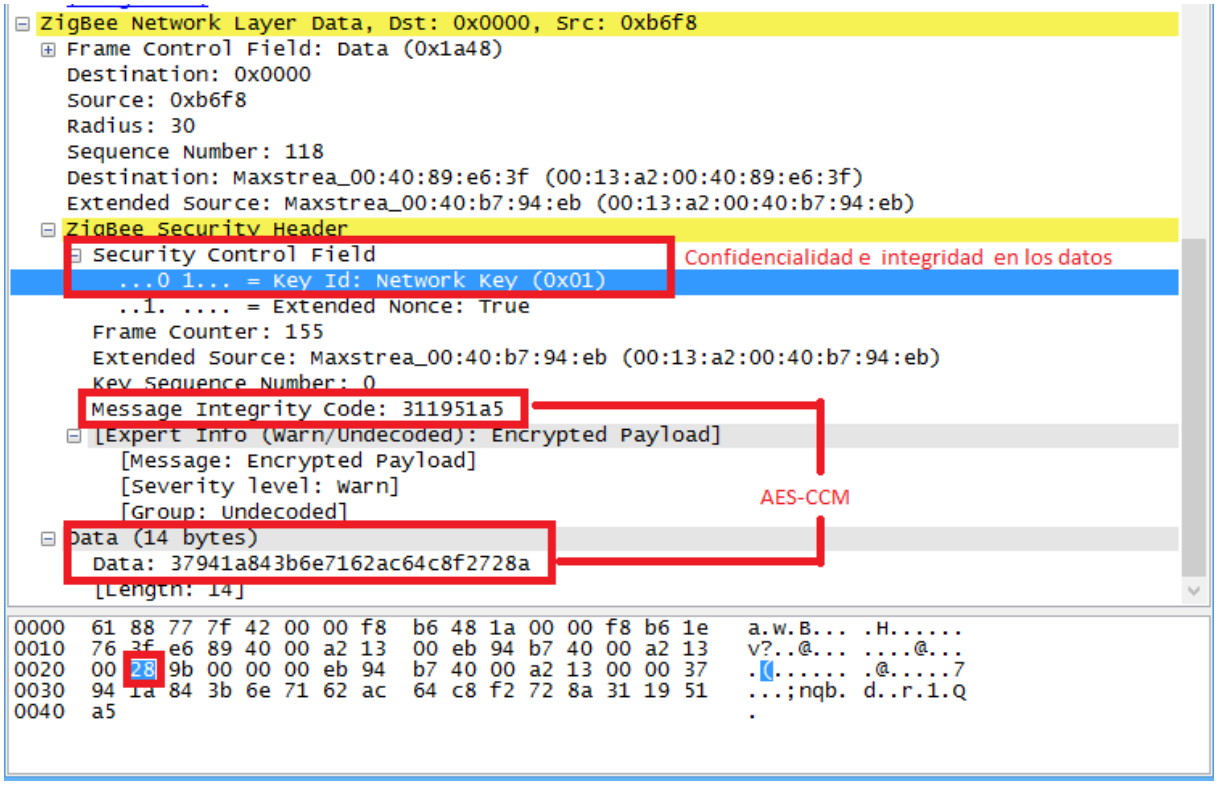


Figura 23. Análisis de los paquetes capturados en Wireshark con el nodo sniffer MC1322x

3.1.3 Desarrollo del aplicativo software Gateway.

El aplicativo software para el *Gateway* desarrollado en javascript sobre nodejs debe capturar la trama proveniente del nodo coordinador y obtener la información proveniente de los datos. Los requisitos de este aplicativo software consisten en realizar la lectura de los datos que llegan al puerto serial provenientes del nodo XBEE y el respectivo envió de los datos cifrados hacia una base de datos. Para el desarrollo del software se analizó la estructura del código y las vulnerabilidades de las librerías utilizadas.

En la primera parte del aplicativo software se utilizó la librería serialport para la lectura del puerto serial y xbee-api para la lectura de las tramas provenientes del modo API donde se realizó un filtrado por capa MAC para solo aceptar información del nodo que está conectado dentro de la misma red del nodo coordinador. En el caso que exista suplantación del nodo router este debe romper los mecanismos de integridad y autenticación realizados en la configuración previa a los nodos. A continuación en la figura 24 se presenta parte del código

fuente desarrollado en javascript y en la figura 25 se presenta la captura de los datos provenientes del nodo sensor.

```
var fs = require('fs');
var request = require("request");

var https = require('https');
var options = {
    key: fs.readFileSync('server-key.pem'),
    cert: fs.readFileSync('server-crt.pem'),
    ca: fs.readFileSync('ca-crt.pem'),
};
var rsp = require('serialport');
var xbee = require('xbee');
var crypto = require('crypto');
var SerialPort = rsp.SerialPort;
var xbeeExplorerDevice = 'COM8';
var temperaturaSensorAddress = '0013a20040b794eb';
var temperaturaFilePath = 'tempalmacenar.csv';
var temperatura=0;
var temperaturacifrada=0;
var  temperaturacifradar=0;
var serial_xbee = new SerialPort(xbeeExplorerDevice, {
  parser: xbee.packetParser()
});

serial_xbee.on('data', function(data) {
    if (data.remote64.hex === temperaturaSensorAddress) {
        temperatura=(((data.analogSamples[0]*256 + data.analogSamples[1])/1023)*1.2*3*100-273.15).toFixed(2);

        var voltage = ((data.samples.supply*1200/1023)/1000).toFixed(1);
        var now = new Date();
        fs.appendFile(temperaturaFilePath,now.toLocaleString()+';'+temperatura+';'+voltage+'\n',function (error) {
            if (error) {
                console.log ('Error, could not write file %s',temperatureFilePath);
                throw err;
            }
        });
```

Figura 24. Parte del código para la lectura de los datos XBEE.

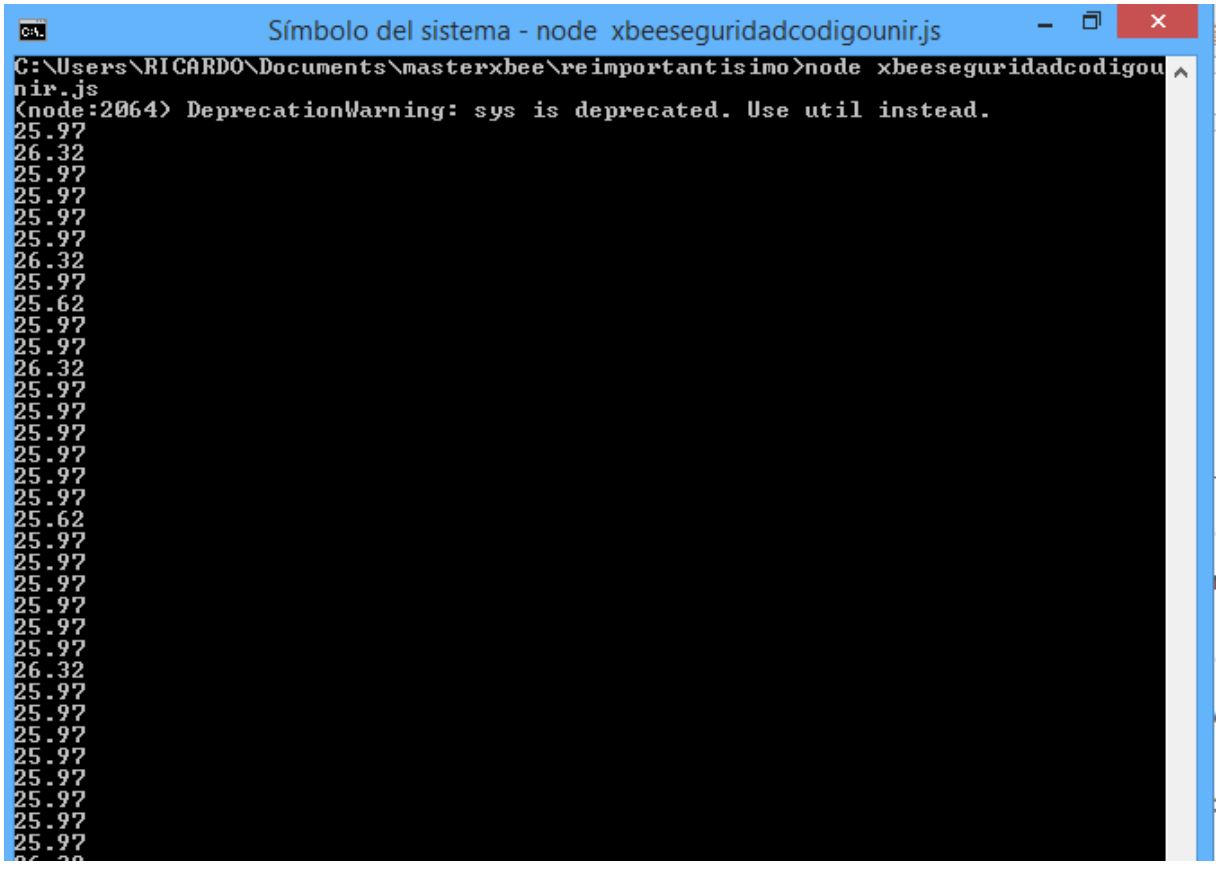


Figura 25. Captura de la temperatura obtenida por el nodo sensor.

Seguidamente en las pruebas preliminares se incluyó al código la creación de un servidor https para el envío de la información de forma cifrada de acuerdo a las peticiones realizadas por el usuario de la red de área local. Para realizar esto fue necesario utilizar la librería https, y la creación de los certificados se realizó utilizando la herramienta OPENSSL.

3.2 Generación de los certificados

Para ofrecer una conexión segura con aplicativo software del Gateway local se generaron los certificados con OPENSSL.

Con OPENSSL primeramente se generó la clave privada. Posteriormente se generó la petición de firma del certificado y por último se generó el certificado SSL. En la figura 26 se presenta el comando para la generación de la clave privada.

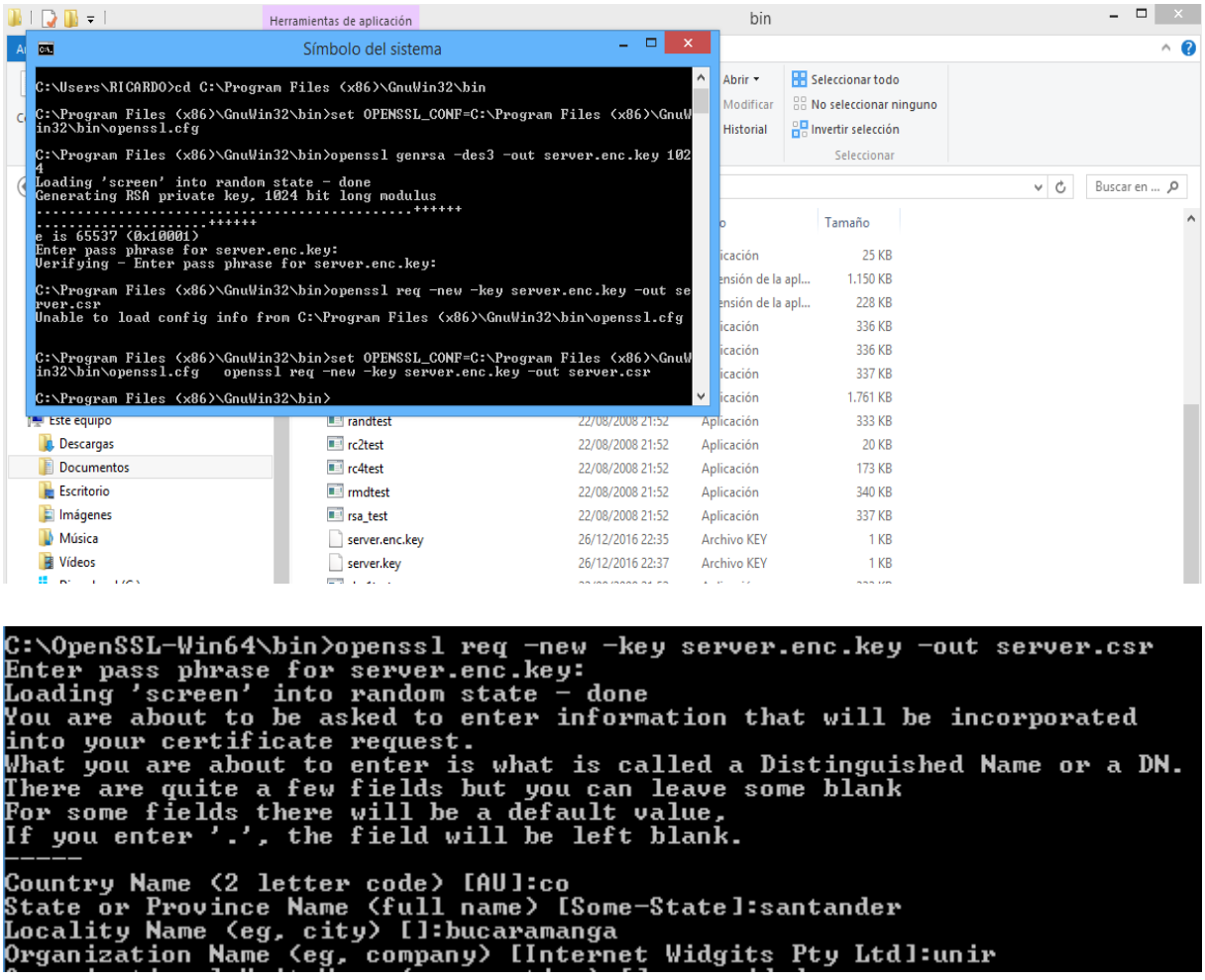


Figura 26. Utilización de openssl para la generación de los certificados.

A continuación en la figura 27 se presenta la clave privada generada con la herramienta OPENSSL.

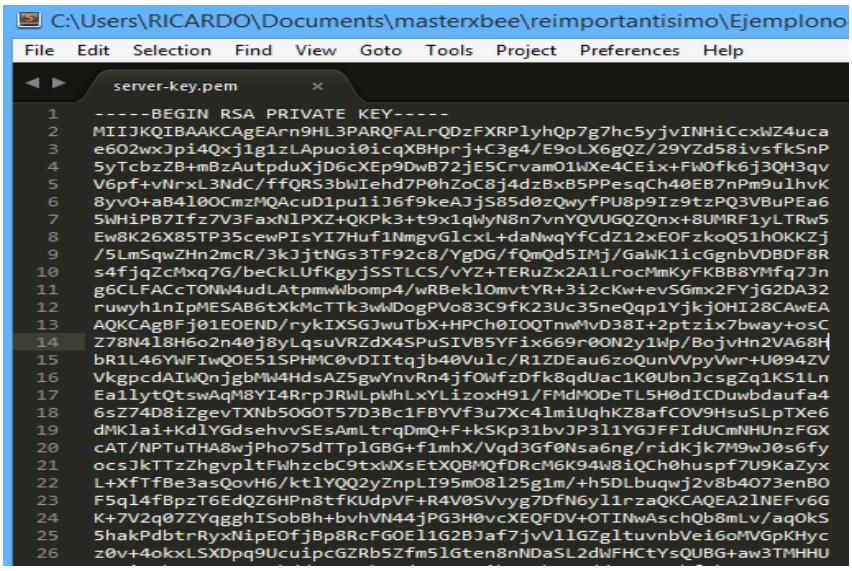


Figura 27. Clave privada RSA elaborada con OPENSSL

También fueron generados los respectivos certificados los cuales se presentan en la figura 28.

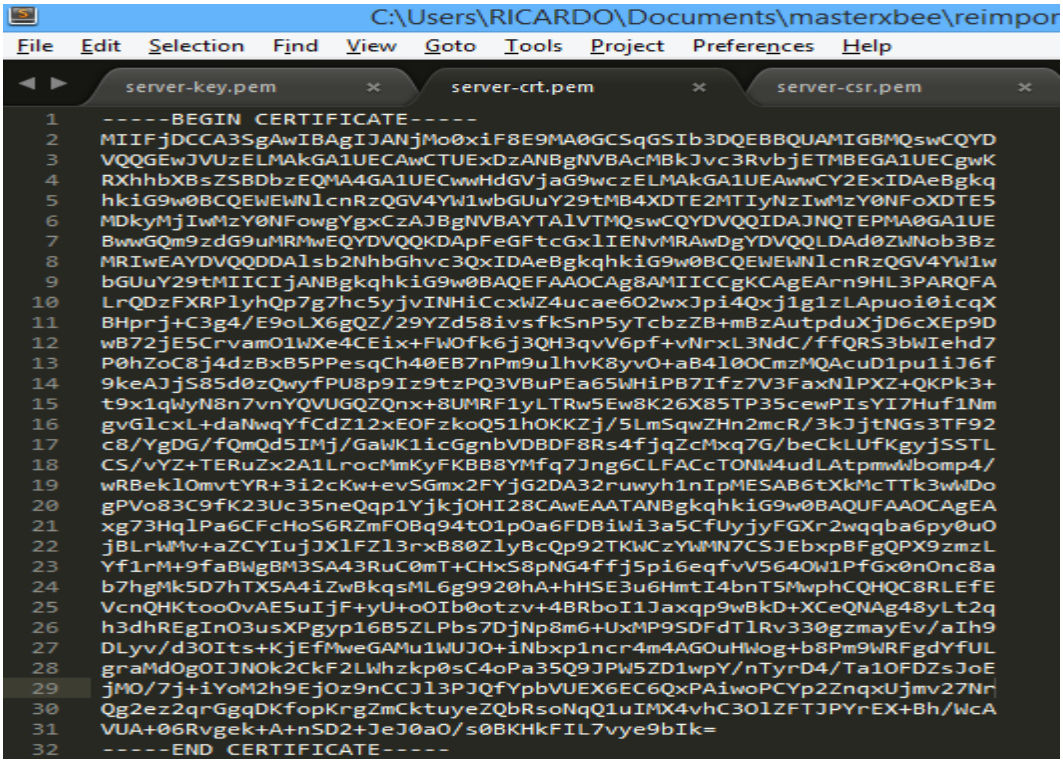


Figura 28. Certificado generado con la herramienta openssl.

Estos certificados son utilizados en el servidor local https desarrollado en javascript el cual se puede validar cuando se accede desde un navegador donde se garantiza que la conexión es

segura. En la figura 29 se presenta la conexión segura al servidor https el cual está obteniendo los datos del nodo xbee coordinador.

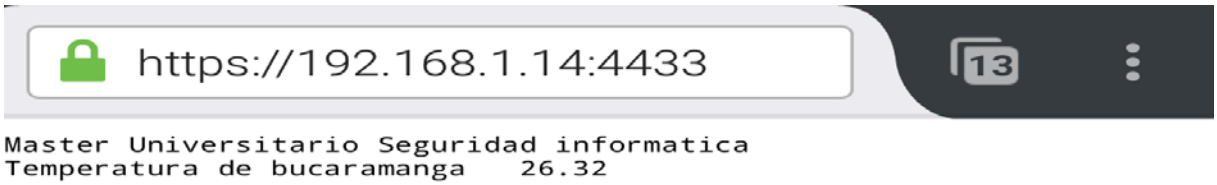


Figura 29. Acceso al servidor https

La conexión segura también se validó utilizando *wireshark,* donde en los datos de la interfaz de red inalámbrica se puede visualizar que la conexión de la capa de transporte se realiza sobre TLSv1.2. En la figura 30 se presentan las capturas de los paquetes de red utilizando *wireshark* donde se puede encontrar que la comunicación de los datos está cifrada.

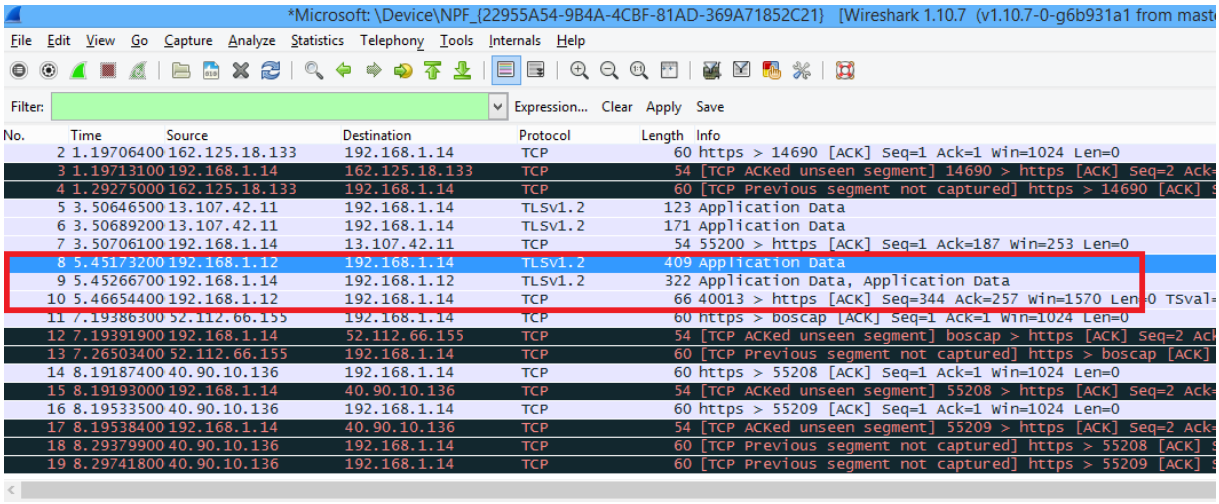


Figura 30 Captura de los paquetes de red cuando se accede al servidor local https

Seguidamente se realizaron pruebas de conexión realizando peticiones a partir de un programa cliente realizado en javascript el cual accede a la conexión https desde una conexión TLS.

Despues se realizó el envío de los datos de temperatura cifrados desde el aplicativo elaborado en javascript con nodejs a la base de datos local en postgresql utilizando la librería crypto y cifrado AES. En la figura 31 se presentan los datos que están cifrados y se están almacenando en la bases de datos.

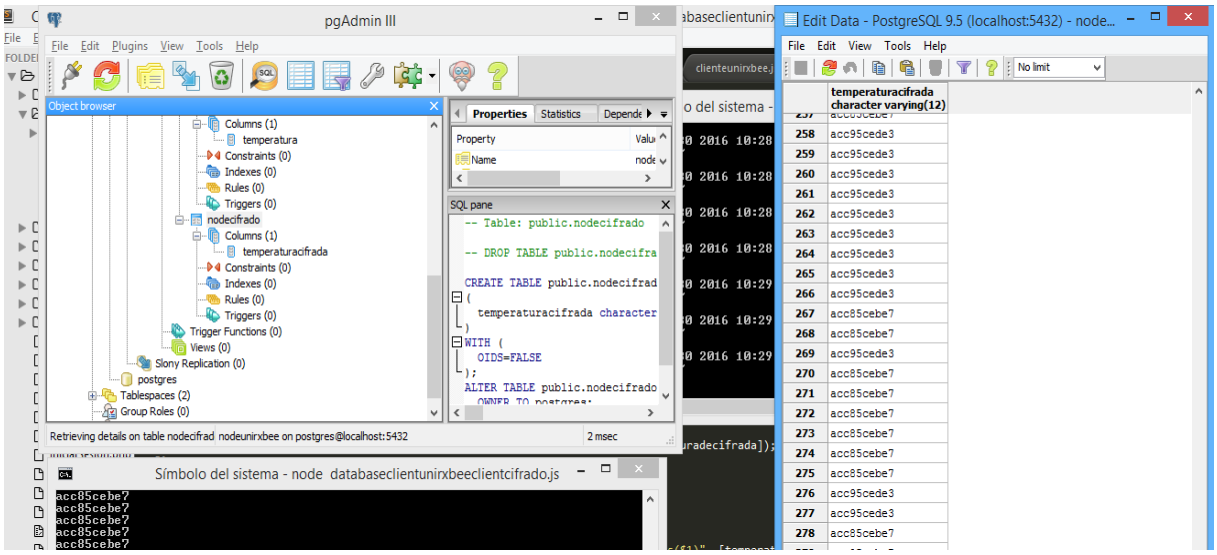


Figura 31. Datos cifrados en javascript y almacenados en postgresql

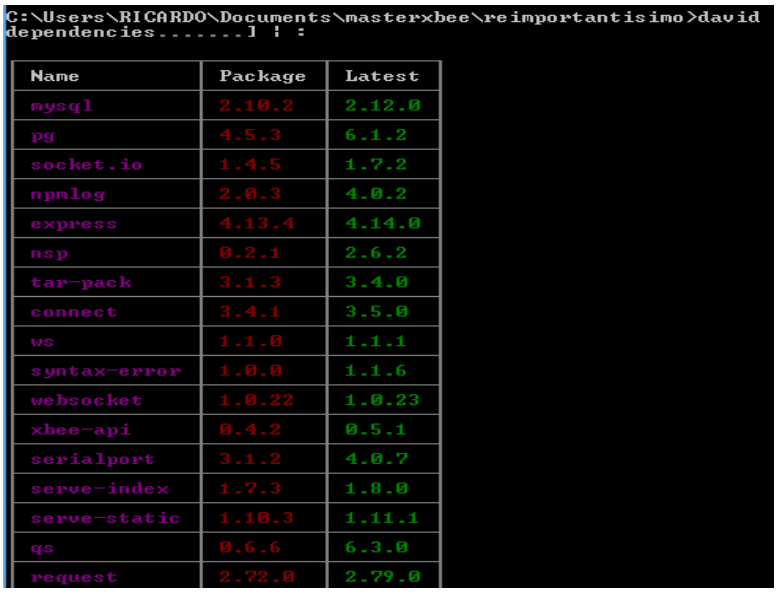
3.3 Vulnerabilidades en nodejs

Para considerar las vulnerabilidades que se puedan generar con el uso de estas librerías se utilizó la herramienta nsp que tiene nodejs, la cual permite revisar los módulos instalados en node.js contra las vulnerabilidades conocidas en la base de datos de nodesecurityio. A continuación en la figura 32 se presentan con el comando *outdated* el cual realiza un cuadro comparativo de las versiones con que cuenta, los paquetes de las librerías que se están utilizando con node.js.

```
C:\Users\RICARDO\Documents\masterxbee\reimportantisimo>npm outdated
Package        Current  Wanted  Latest  Location
connect          3.4.1   3.5.0   3.5.0
express         4.13.4  4.14.0  4.14.0
mysql           2.10.2  2.12.0  2.12.0
npmlog           2.0.3   2.0.4   4.0.2
pg               4.5.3   6.1.2   6.1.2
request         2.72.0  2.79.0  2.79.0
serialport       3.1.2   4.0.7   4.0.7
serve-index      1.7.3   1.8.0   1.8.0
serve-static    1.10.3  1.11.1  1.11.1
socket.io        1.4.5   1.7.2   1.7.2
tar-pack         3.1.3   3.1.4   3.4.0
websocket        1.0.22  1.0.23  1.0.23
ws               1.1.0   1.1.1   1.1.1
xbee-api         0.4.2   0.5.1   0.5.1
```

Figura 32. Versiones de los Paquetes utilizados.

También se utilizó el modulo David para evaluar si las librerías que se están utilizando se encuentran desactualizadas. En la figura 33 se presentan los paquetes que se están utilizando para el desarrollo del software.



```
C:\Users\RICARDO\Documents\masterxbee\reimportantisimo>david
dependencies.......] | :
```

Name	Package	Latest
mysql	2.10.2	2.12.0
pg	4.5.3	6.1.2
socket.io	1.4.5	1.7.2
npmlog	2.0.3	4.0.2
express	4.13.4	4.14.0
nsp	0.2.1	2.6.2
tar-pack	3.1.3	3.4.0
connect	3.4.1	3.5.0
ws	1.1.0	1.1.1
syntax-error	1.0.0	1.1.6
websocket	1.0.22	1.0.23
xbee-api	0.4.2	0.5.1
serialport	3.1.2	4.0.7
serve-index	1.7.3	1.8.0
serve-static	1.10.3	1.11.1
qs	0.6.6	6.3.0
request	2.72.0	2.79.0

Figura 33. Paquetes de nodejs utilizados para el desarrollo del software.

3.4 Desarrollo del Aplicativo WEB

Se elaboró un aplicativo software en php utilizando el aplicativo software postgreSQL PHPgenerator y el código de descifrado utilizado es AES-128.

El software permite de forma rápida eficiente y segura crear un entorno WEB para la visualización de la información alojada en la base de datos. A continuación en la figura 34 se presenta el *framework* de phpgenerator.

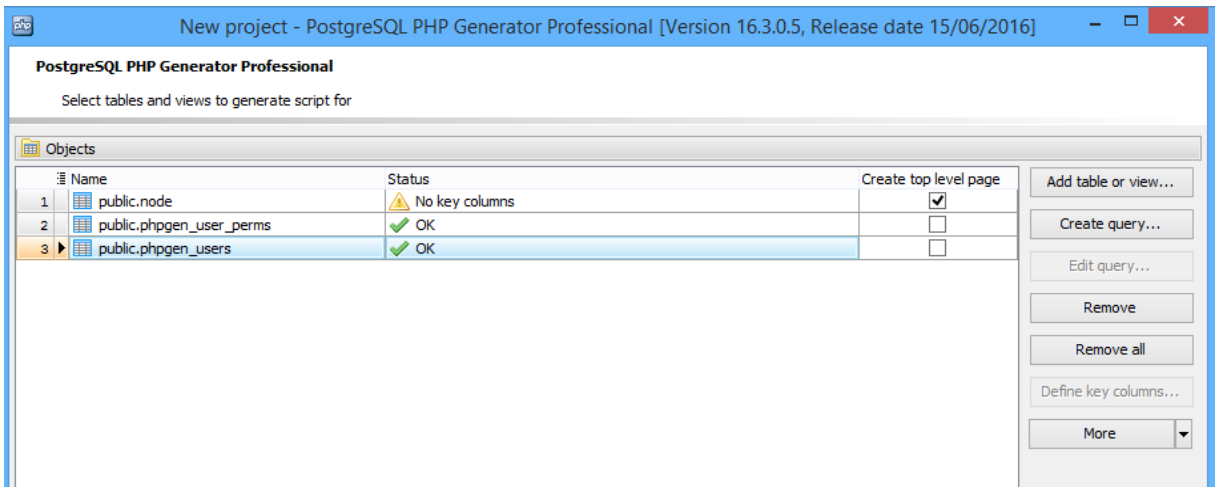


Figura 34. Interfaz de PostgreSQL php generator para la generación del aplicativo WEB.

Después se seleccionó la interfaz gráfica para la visualización de los datos dentro del aplicativo web. En la figura 35 se presentan los temas de interfaz para la visualización de los datos presentes en la base de datos.

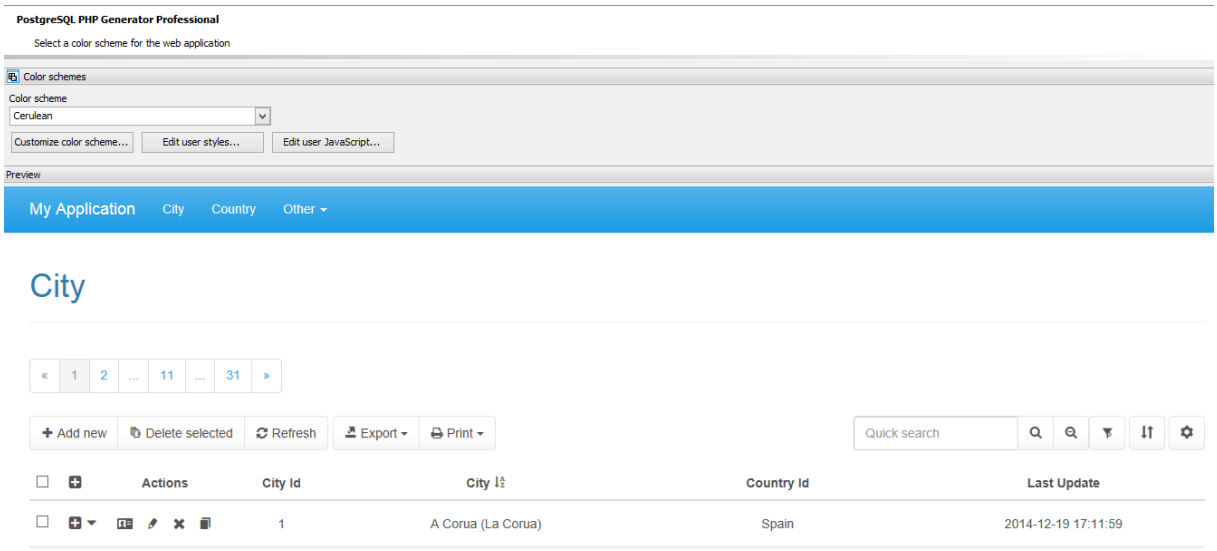


Figura 35. Selección de los temas PostgreSQL php generator

Finalmente se habilitaron los mecanismos de seguridad y la gestión de los permisos para los usuarios que tengan acceso al aplicativo WEB. En la figura 36 se presenta la configuración de la tabla de autorización de acceso para los usuarios al aplicativo WEB.

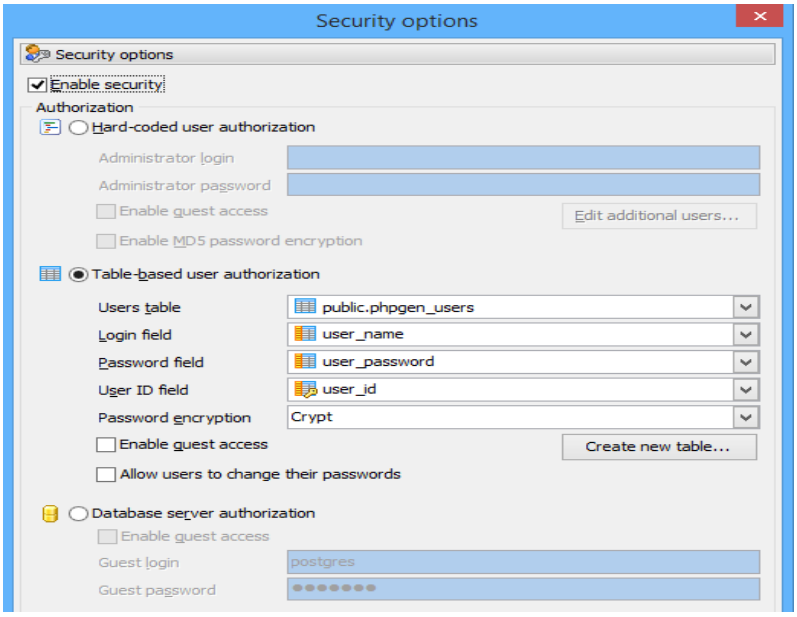


Figura 36. Opciones de seguridad para el acceso al aplicativo WEB.

Para utilizar el aplicativo WEB generado se elaboraron las tablas en postgresql utilizando phppgadmin. En la figura 37 se presenta la base de datos alojada en el *hosting*.

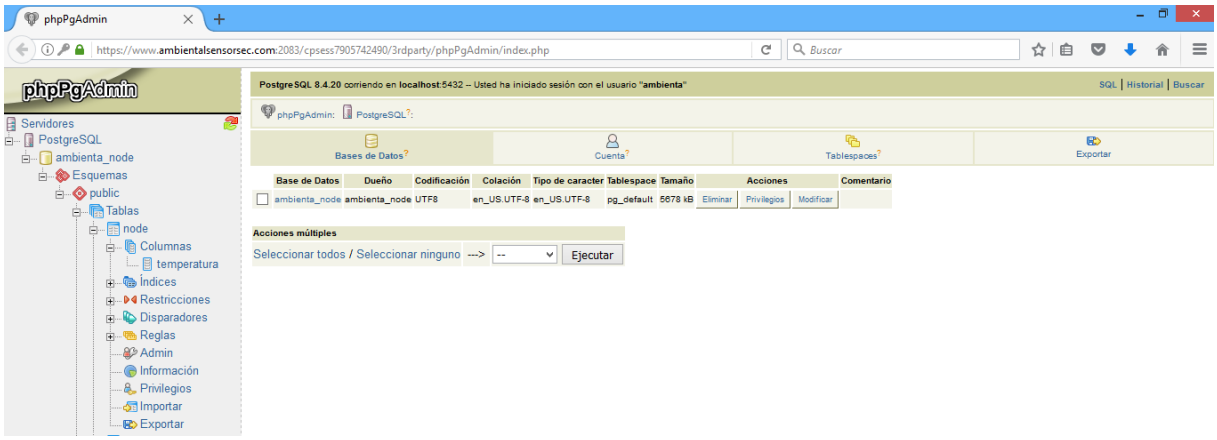


Figura 37. Base de datos alojado en el hosting.

3.4.1 Mecanismos de seguridad en el hosting Cpanel.

El cpanel permite administrar archivos y gestionar diversos recursos .En la figura 37 se presentan la gestión de los recursos de seguridad que permite CPANEL. Entre las principales características están: Control de conexiones por SSH, bloqueo el acceso por IP, permite protección por enlace directo evitando que se incorpore contenido del sitio WEB en otro sitio, protección *leech* para evitar que un usuario que publique su login y contraseña de forma errónea pueda ser utilizada para acceder a zona restringidas dentro de los directorios y permite configurar SSL para conexiones seguras. En la figura 38 se presentan las opciones para la gestión de seguridad que se encuentran dentro del CPANEL.

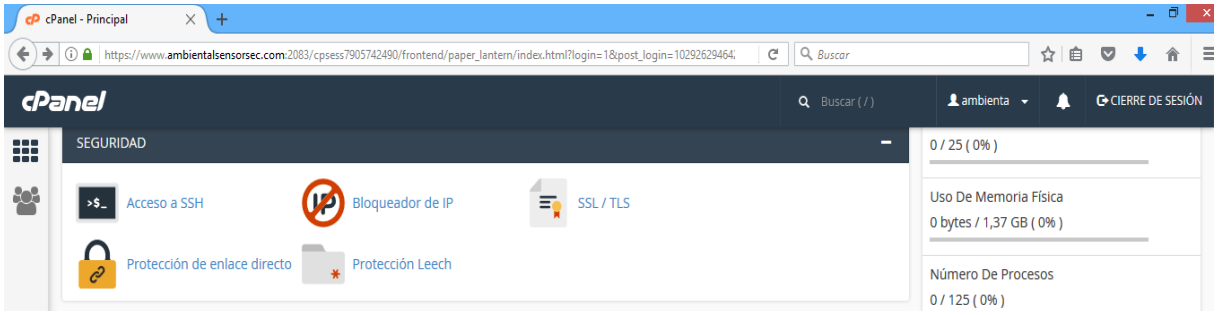


Figura 38. Gestión de los recursos de seguridad

En el envío cifrado de la información se utilizó la opción SSL/TLS. Para garantizar la conexión segura SSL se configuró la clave privada para descifrar la información transmitida y enviada hacia el *hosting* en la figura 39 se presenta la interfaz del CPANEL.

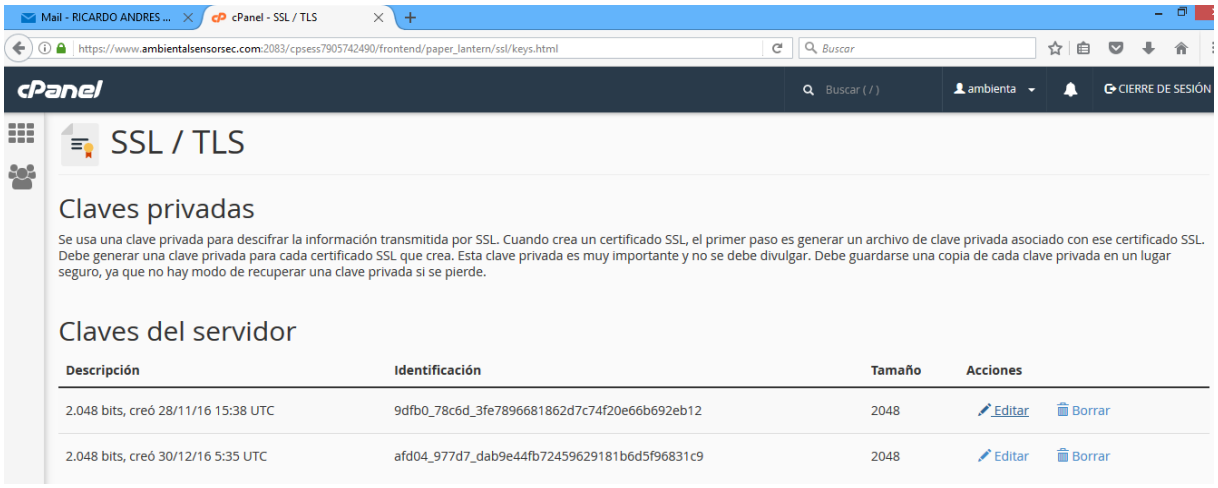


Figura 39. Interfaz para la generación de la clave privada asociada al certificado SSL.

Seguidamente se aloja un certificado de confianza para el sitio WEB donde se coloca la página. La autoridad certificadora es *Lets Encrypt*. En la figura 40 se presenta la interfaz para colocar el certificado SSL para el sitio WEB.

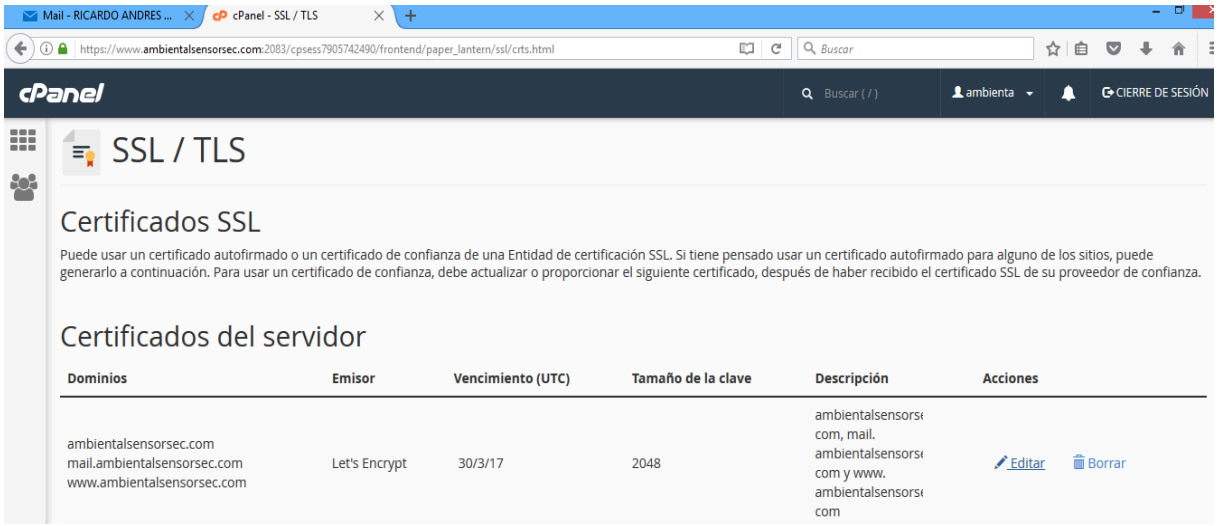


Figura 40. Interfaz CPANEL para alojar el certificado SSL

3.4.2 Interfaz del aplicativo WEB

Cuando se accede al aplicativo se encuentra un panel frontal que es el que permite acceder a la plataforma web de visualización de los datos provenientes de la red de sensores XBEE.

(El aplicativo está alojado en un *hosting* que se administra con CPANEL). A continuación en la figura 41 se presenta el ingreso al aplicativo WEB elaborado.

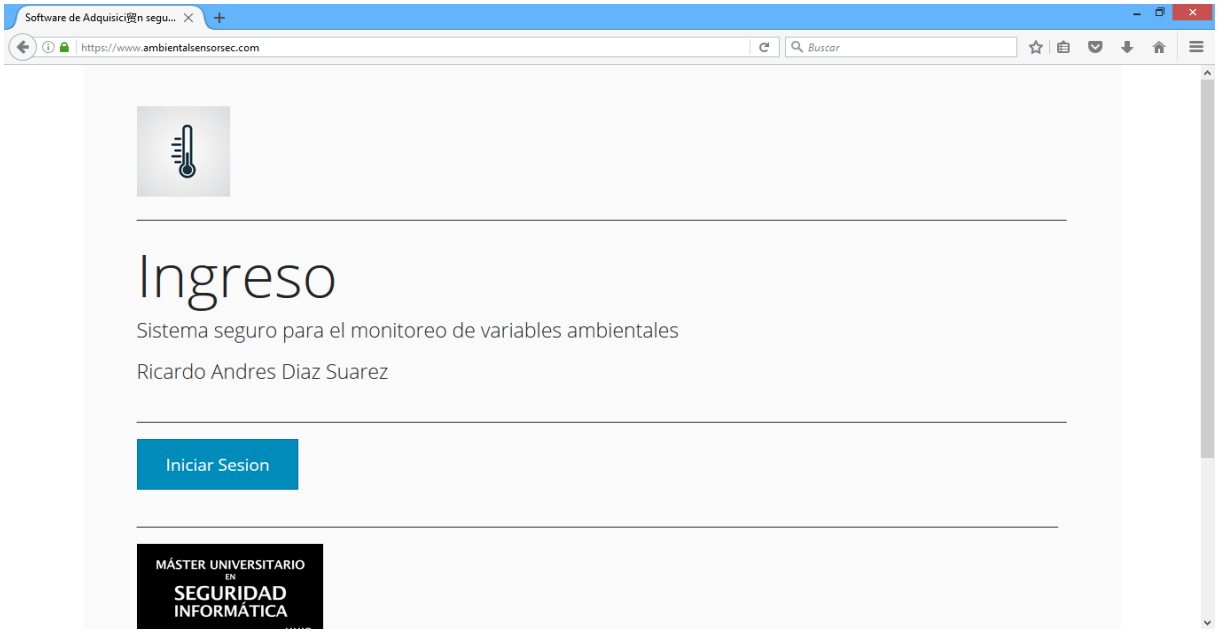


Figura 41. Plataforma de ingreso al aplicativo WEB elaborado conexión https.

Después del panel principal se pasa a una interfaz de acceso en la cual el usuario debe tener el *username* y el *password*. En la figura 42 se presenta la interfaz de acceso de usuario con envío de datos cifrados.

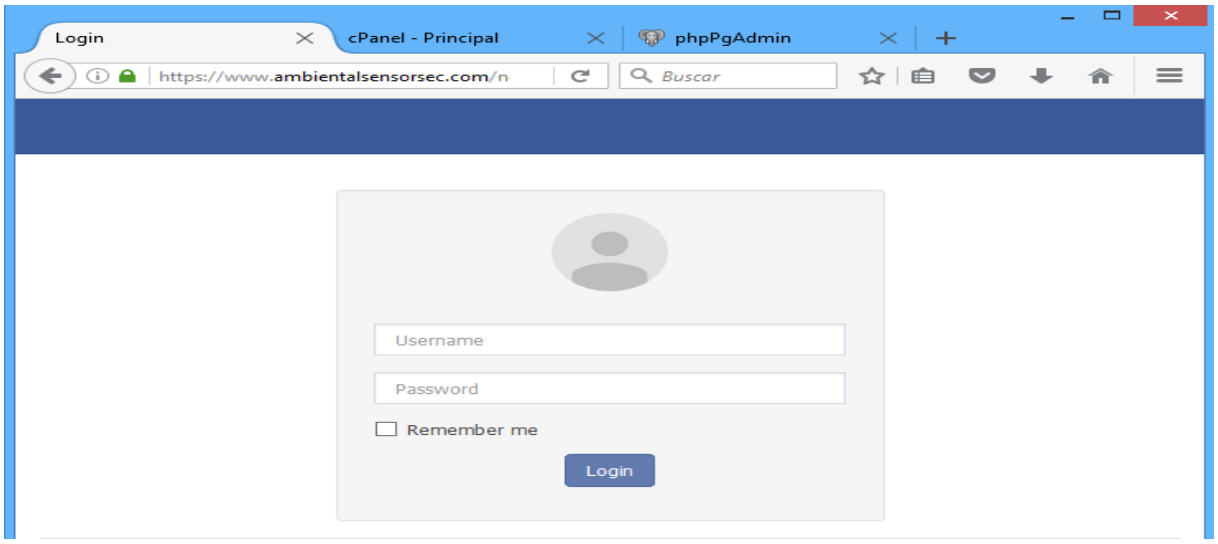


Figura 42. Panel de acceso del aplicativo WEB.

El usuario después de llenar sus datos pasa a la interfaz del aplicativo WEB donde puede visualizar la información proveniente del nodo sensor. Estos datos llegaron cifrados desde el Gateway AES y esta conexión se realiza cifrada desde el Gateway hasta el *hosting* remoto. En la figura 43 se presenta la información presentada del aplicativo WEB.

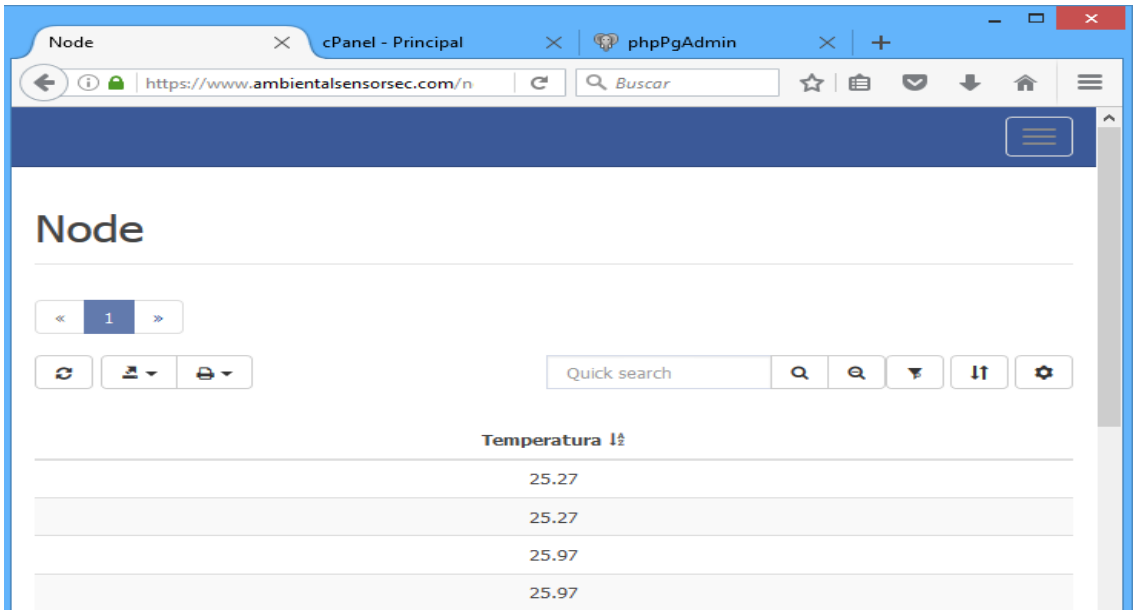


Figura 43. Interfaz del aplicativo WEB elaborado.

En la figura 44 se presenta el código en PHP que realiza el proceso de descifrado de la información proveniente del código elaborado en javascript que captura la información del nodo la cifra utilizando AES-128 y la envía utilizando una conexión TLS con el *hosting* remoto.

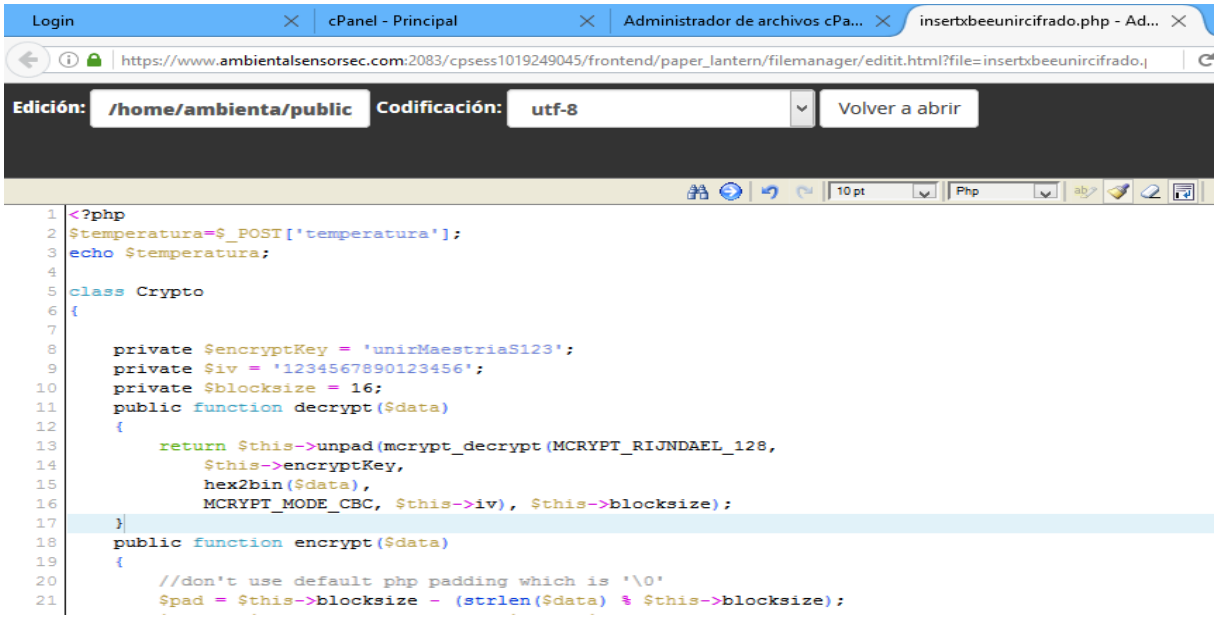


Figura 44. Código que realiza el proceso de descifrado.

Para evaluar que la comunicación entre los datos se encuentra cifrada entre la información proveniente del Gateway y el *hosting* remoto se utilizó la herramienta *wireshark.* Primero se encontró la dirección IP del *hosting* adquirido. En la figura 45 se presenta la dirección IP del *hosting* que se implementó para el desarrollo del prototipo.

Figura 45. Dirección IP del hosting.

En la figura 46 se presenta la captura en *Wireshark* donde se presenta la captura de los paquetes enviados entre el *Gateway* y el *hosting* remoto. Se puede evidenciar que los datos están cifrados y el protocolo que se utiliza es TLSv1.2.

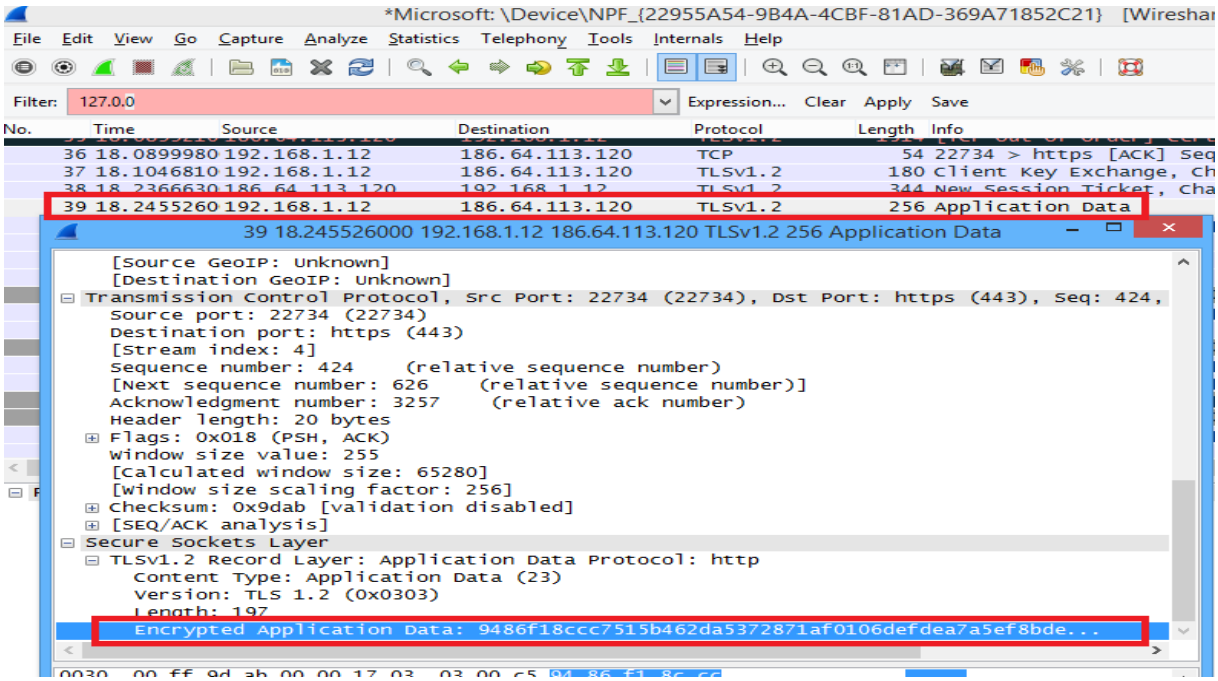


Figura 46. Captura del tráfico entre el Gateway y el hosting remoto.

4. Conclusiones.

Se construyó un estado del arte para identificar las diferentes vulnerabilidades presentes en las redes de sensores inalámbricos los diferentes tipos de ataques y los posibles mecanismos de seguridad que pueden ser implementados para solventar este tipo de vulnerabilidades.

Dentro de la elaboración del marco teórico se identificaron las diferentes características del estándar IEEE802.15.4 en cuanto a la seguridad de los paquetes. Con los campos *auxiliary security header.*

Se desarrolló una red con radios XBEE utilizando cifrando y MIC para garantizar la confiabilidad e integridad de la información enviada por los nodos. Esto se pudo comprobar utilizando el radio MCX1322 y el aplicativo software *wireshark*.

Se elaboró un aplicativo software utilizando javascript que corre sobre nodejs que permite establecer una conexión TLS y realiza el proceso de cifrado de los datos enviados por la red de sensores utilizando el algoritmo de cifrado AES 128 bits y la librería crypto. El proceso de descifrado se realizó en un código elaborado en PHP.

El aplicativo web se encuentra en un *hosting* de conexión segura https para garantizando la confiabilidad e integridad de los datos que pueden ser visualizados dentro del aplicativo web.

Se evaluó que las transmisiones provenientes desde los nodos hasta el servidor remoto se encuentran cifradas desde el nodo router hasta que se envía hasta el *hosting* remoto http://www.ambientalsensorsec.com/.

Se deben incluir nodos XBEE *sniffer* para monitorizar la presencia de nodos intrusos o cambios del funcionamiento de la red esto permitiría tener mecanismo de seguridad respecto a ataques físicos o ataques tipo sink hole.

Para el desarrollo de trabajos futuros se deben utilizar mecanismos de cifrado adicionales sobre el sistema operativo del radio Zigbee y evaluar su desempeño.

5 Bibliografía.

Adrian Perrig, R. S. (2001). SPINS: Security Protocols for Sensor Networks . *Memorias Mobile Computing and Networking* , 1-11.

Alvaro Diaz Suárez, P. S. (2014). *Plataforma virtual para el análisis del rendimiento y la seguridad en redes de sensores inalámbricas.* Cantabria: Facultad de Ciencias-Universidad de Cantabria.

Carbajal, E. E. (2012). *Redes de sensores inalambricas aplicada a la medicina.* Comunidad autonoma de cantabria: Universidad de Cantabria.

Carlos Garcia Arano, D. A. (2010). *Impacto de la seguridad en las redes inalambricas de sensores IEEE 802.15.4.* España: Universidad complutense de Madrid.

Diana Milena Archila Córdoba, F. A. (2013). Estado del arte de las redes de sensores inalambricos. *Revista digital TIA*, 4-15.

Faludi, R. (2010). *Building Wireless sensor Networks.* O'Relly.

Free Scale. (2010). *1322x USB Dongle Reference Manual .* Arizona: Free scale semiconductor.

IEEE Standards Associations. (2015). *IEEE Standar for Low-Rate Wireless Networks.* Estados Unidos: IEEE.

ITU-T. (2014). *Applications of Wireless Sensor Networks in next generation networks.* International : Technical paper Telecommunication standardization sector of ITU.

jbthomsen. (2016, 8 10). Retrieved from https://github.com/jbthomsen/WiresharkZigbeeUtility: https://github.com/jbthomsen/WiresharkZigbeeUtility

Jimena Garbarino, A. E. (2011). *Protocolos para redes inalámbricas de sensores.* Buenos Aires Argentina: Universidad de Buenos Aires .

Jorge Pablo Dignani, F. G. (2011). *Analisis del protocolo Zigbee.* Ciudad de la plata: Universidad Nacional de la plata .

Libelium. (2016, 10 10). *http://www.libelium.com/security-802-15-4-zigbee/*. Retrieved from http://www.libelium.com/security-802-15-4-zigbee/: http://www.libelium.com

Madhukar Anand, E. C. (2006). Sensor Network Security: More Interesting Than You Think . *Penn Libraries*, 1-5.

Martínez, B. O. (2015). *Seguridad en redes de sensores inalámbricos basados en funciones físicamente no-clonables.* Ciudad de Mexico: Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional.

NIST. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems .* USA: National institute of standards and technology.

Perez Juan, U. E. (2014). Metodología para el diseño de una red de sensores inalámbricos . *Universidad, Ciencia y Tecnología*, 12-22.

Roberto Fernández Martínez, J. O. (2009). *Redes inalámbrica de sensores: teoría y aplicacion práctica.* España: Universidad de la rioja servicio de publicaciones.

Silicon Laboratories. (2013). The evolution of the wireless sensor networks. *Silicon Labs*, 1-5.

Suescún, C. A. (2009). Seguridad en redes de sensores inalámbricos . *Sistemas & telematica* , 43-73.