ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

EVALUACIÓN DE EFICIENCIA ENERGÉTICA EN LAS COMUNICACIONES ENCRIPTADAS DE UNA RED DE SENSORES INALÁMBRICOS (WSN) QUE MONITORIZA ONDAS SÍSMICAS

TRABAJO DE TITULACIÓN
Tipo: **PROPUESTA TÉCNICA**

Para optar al Grado Académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTORES: ÍTALO FERNANDO PARREÑO SAÑICELA
ANDRÉS MAURICIO SOLÍS GOYES

TUTOR: ING. ALBERTO ARELLANO AUCANCELA MSc.

Riobamba –Ecuador

2019

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: La propuesta técnica: "EVALUACIÓN DE EFICIENCIA ENERGÉTICA EN LAS COMUNICACIONES ENCRIPTADAS DE UNA RED DE SENSORES INALÁMBRICOS (WSN) QUE MONITORIZA ONDAS SÍSMICAS", de responsabilidad de los señores ítalo Fernando Parreño Sañicela y Andrés Mauricio Solís Goyes, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

Ing. Washington Luna **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Patricio Romero **DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Alberto Arellano MSc. **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Diego Veloz MSc. **MIEMBRO DEL TRIBUNAL**	_____	_____

Nosotros, ítalo Fernando Parreño Sañicela y Andrés Mauricio Solís Goyes somos responsables de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo.

Ítalo Fernando Parreño Sañicela
Andrés Mauricio Solís Goyes

DEDICATORIA

El siguiente trabajo de titulación está dedicado a Dios y la Virgen de la Nube, que me han dado la vida y la sabiduría en mis estudios, a mis padres, Alicia Sañicela y Fernando Parreño que por ellos estoy aquí, fueron el apoyo durante mi vida, me guiaron en mis estudios, por sus palabras de apoyo y su cariño. A mi madrina Laurita Orozco por sus consejos, su forma de guiar mi vida. A Jesenia Oña y, por último, pero no menos importante a mis amig@s y demás familiares que me brindaron su apoyo.

Ítalo Parreño S.

Este trabajo de titulación va dedicado a mi madre Ximena Goyes y mi padre Gonzalo Solís por el amor, la sabiduría y el cariño que me han entregado que han sido mi guía durante toda mi vida. A mi Abuelita Charito y a mi abuelita Lupita por todo el cariño que me han entregado, la sabiduría de sus palabras y los consejos que me brindaron en cada momento.

Andrés Solís Goyes

AGRADECIMIENTO

Agradezco a Dios y a la Virgen de la Nube por cuidarme y protegerme durante mi vida estudiantil, a mis padres que me dieron su apoyo y confianza. Al Ing. Alberto Arellano por su guía y asesoramiento en el desarrollo de este trabajo de titulación. A la Escuela Superior Politécnica de Chimborazo, por permitirme formarme académicamente, a los profesores que, durante todo este camino académico, compartieron sus experiencias y conocimientos, para formarme como un profesional con las destrezas y valores que este mundo competitivo exige. A todas aquellas personas que formaron parte de este camino, que aportaron de una manera directa e indirecta para la culminación de mi carrera.

Ítalo Parreño S.

Primeramente, agradeciéndole a Dios por cuidarme, guiarme y protegerme en todo momento, a mis padres por apoyarme siempre y en cada paso que he dado estando en todo momento. A mi abuelita Charito y mi abuelita Lupita quienes han estado siempre al pendiente de mí y me han cuidado siempre. A mi primo Alejandro quien me brindo ayuda y me ha apoyado en todo lo que he necesitado. A Verito por apoyarme y aconsejarme en todo momento. Al Ing. Diego Veloz por la ayuda y el asesoramiento durante el progreso de este trabajo de titulación como también en el desempeño académico. Al Ing. Vinicio Ramos por la guía tanto en materias impartidas como en la academia de redes. A la Escuela Superior Politécnica de Chimborazo por haberme abierto las puertas hacia un camino de éxito y superación personal, así como académica. A mis familiares y amigos que me ayudaron en el camino y para la culminación de la carrera.

Andrés Solís Goyes

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

GPS	Global Positioning System
ADC	Analog-to-Digital Converter
RF	Radio Frequency
WSN	Wireless Sensor Networks
TCP/IP	Transmission Control Protocol/Internet Protocol
IoT	Internet of Things
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
UDP	User Datagram Protocol
PVDF	Polifluoruro de vinilideno
EMI/RFI	ElectroMagnetic Interference/Radio Frequency Interference
CA	Certificación
MANET	Mobile Ad hoc Network
NSA	National Security Agency
DES	Data Encryption Standard
RSA	Rivest, Shamir y Adleman
AES	Advanced Encryption Standard
CPU	Central Processing Unit
MAC	Media Access Control

RESUMEN

El objetivo de este trabajo de titulación fue evaluar la eficiencia energética en las comunicaciones encriptadas de una red de sensores inalámbricos que monitorea ondas sísmicas. Se construyó una maqueta con cinco áreas que simulen el movimiento telúrico, cada área consta de un motor con una centrina adherido a una placa de madera, cada motor posee su respectivo circuito modulador de ancho de pulso (PWM) que permite variar el movimiento de estas placas, cada placa cuenta con un nodo sensor compuesto de una lámina piezoeléctrica que censa los movimientos, una tarjeta Waspmote que procesa las señales del sensor y las encripta, un zigbee que envía la información codificada a un nodo gateway, este recibe toda la información de los cinco nodos sensores, y una batería que alimenta cada nodo. Por las prestaciones que ofrecen las tarjetas se seleccionaron dos tipos de encriptación, simétrica y asimétrica; siendo los algoritmos AES 128, AES 192 y AES 256 correspondientes a encriptación simétrica y RSA a encriptación asimétrica. Para esta evaluación se transmitieron 35 bytes de datos en texto plano, transformándose a 61 bytes con el algoritmo AES en sus tres tipos de longitud de llaves y en 96 bytes con RSA. Se utilizaron tres herramientas de medición: un multímetro Serie 830 y un multímetro RadioShack para el nodo sensor y un medidor Keweisi para el nodo gateway. Se determinó el número de repeticiones del experimento del envió de datos para esta red mediante cálculos estadísticos, proyectando un total de 200 veces. Obteniendo los siguientes datos: texto plano de 77.2 mA, AES 128 de 77.9 mA, AES 192 de 79.6 mA, AES 256 de 79.8 mA y RSA de 81.7 mA, determinando que el algoritmo simétrico AES 128 brinda un equilibrio entre protección de los datos y consumo energético.

PALABRAS CLAVE: <COMUNICACIONES INALÁMBRICAS>, <COMUNICACIÓN ENCRIPTADA>, <ALGORITO SIMÉTRICO>, <ALGORITMO ASIMÉTRICO> <ONDAS SÍSMICAS>, <PIEZOELÉCTRICO>, <WASPMOTE>, <ZIGBEE>.

ABSTRACT

The following investigation's objective was to evaluate the energy efficiency in the encrypted communications of a wireless sensor network that monitors systemic waves. A model with five areas that simulate the telluric movement was built, each area consists of a motor with a centrina attached to a wooden plate, each motor has its respective pulse width modulator circuit (PWM) that allows to vary the movement of these plates, each board has a sensor node composed of a piezoelectric sheet that monitors the movements, a waspmote card that processes the sensor signals and encrypts them, a zigbee that sends the encoded information to a gateway node, it receives all the information from the five sensor nodes, and a battery that feeds each node. For the services offered by the cards, two types of encryption were selected, symmetric and asymmetric; being the algorithms AES128, AES192 and AES 256 corresponding to symmetric encryption and RSA to asymmetric encryption. For this evaluation, 35 bytes of data were transmitted in plain text, being transformed to 61 bytes with the AES algorithm in its three key length types and in 96 bytes with RSA. Three measuring tools were used: a Series 830 multimeter and a RadioShack multimeter for the sensor node and a Keweisi meter for the Gateway node. The number of repetitions of the data sending experiment for this network was determined by statistical calculations, projecting a total of 200 times. Obtaining the following data: 77.2m A, a flat text AES 128 of 77.9mA, AES 192 of 79.6mA, AES256 of 79.8mAy and RSA of 81.7mA, determining that the symmetric algorithm AES 128 provides a balance between data protection and consumption energetic.

KEYWORDS: <WIRELESS COMMUNICATIONS>, <ENCRYPTED COMMUNICATION>, <SYMMETRIC ALGORITE>, <ASYMMETRIC ALGORITHM> <SYSTEMIC WAVES>, <PIEZOELECTRIC>, <WASPMOTE>, <ZIGBEE>.

INTRODUCCIÓN

ANTECEDENTES

En los últimos años, las Wireless Sensor Networks (WSN) han llamado la atención en el área de investigación. Una WSN consiste en una gran cantidad de sensores de diferentes tipos que pueden monitorear una amplia variedad de condiciones ambientales tales como temperatura, humedad, movimiento vehicular, presión, niveles de ruido, etc. Los sensores al tener un bajo costo nos permiten desplegar una gran cantidad de ellos para realizar aplicaciones militares y civiles.

Sin embargo, la ventaja presente en el costo de los sensores también conduce a graves limitaciones de recursos, como la energía de la batería, la memoria y baja capacidad de computación, y estas restricciones a su vez presentan importantes obstáculos para la implementación de los enfoques tradicionales de seguridad informática (como la clave pública). (Rocabado, 2013)

La naturaleza abierta y la operación desatendida de las WSN hacen que las defensas de seguridad sean aún más difíciles. Debido a esto los problemas de seguridad que presentan las redes WSN son la administración de claves, autenticación de mensajes, detección de intrusos, etc. Sin embargo, a pesar de la topología de red estática, los WSN tradicionales presentan los siguientes inconvenientes:

- Los sensores Near-Sink drenan su energía más rápido que otros sensores en la red porque estos sensores no solo deben entregar sus propios datos al receptor, sino también reenviar datos que provienen de muchos otros sensores.
- En áreas hostiles para seres humanos, como campos de batalla, áreas volcánicas, zonas submarinas, etc., los sensores generalmente se despliegan en aviones o helicópteros, lo que crea la difícil ubicación del sensor e incertidumbre en la cobertura.
- Además, en las áreas mencionadas anteriormente, puede que no ser factible desplegar un receptor fijo (o estación base).

Este tipo de redes al ser de la categoría inalámbrica es muy susceptible a diferentes ataques, pudiendo ser de las siguientes naturalezas:

- Ataques Externos

  Debido a la naturaleza abierta de las comunicaciones inalámbricas, los participantes no autorizados de la red pueden espiar la frecuencia de radio de los WSN. Por ejemplo, en una aplicación de campo de batalla, los sensores se utilizan para detectar ruido, vibración y luz causados por el movimiento de tropas. Un adversario puede alterar o falsificar paquetes para inducir inexactitudes.

- Ataques Internos

  Suceden cuando los sensores autorizados de los WSN se comportan de forma involuntaria o no autorizada. Cuando los sensores son capturados, el adversario puede realizar ataques a información privilegiada como la generación de datos falsos, que buscan robar secretos de la red e interrumpir su funcionamiento normal.

Varios trabajos en ramas similares, estudiadas en diferentes escenarios, lugares y condiciones, a continuación, serán descritos permitiéndonos así conocer los resultados de estas investigaciones.

"Integración Segura de MANETs con Limitaciones de Energía a Redes de Infraestructura". (CACIC 2011, La Plata - Buenos Aires - Argentina.) En este trabajo, el estudio realizado fue un caso de integración de una MANET Bluetooth indoor a una red de infraestructura, sin considerar condiciones externas como distancia, interferencias y otras. Para el punto de acceso de la red se implementó utilizando las características de enrutamiento de Linux, habilitando la pila de protocolos BlueZ.

Se efectuaron mediciones extremo a extremo sobre un canal "no seguro" y luego sobre un canal "seguro", para asegurar el canal se implementó utilizando diferentes configuraciones del protocolo IPSec.

En otra investigación realizada, esta vez sobre un escenario de pruebas outdoor el cual se ve afectado por factores externos que disminuyen el rendimiento y por ello el consumo de recursos en los nodos de la red Ad Hoc se incrementan. En el desarrollo de la investigación, Bluetooth es la tecnología de soporte para la formación de la MANET remota y de GSM/GPRS para la integración de la misma red de infraestructura. El consumo de energía para cada configuración de canal y la distribución de energía en el trabajo han sido analizados bajo los siguientes ítems: Establecimientos de sesión, encriptación, autenticación y transmisión.

Sergio Rocabado al realizar su caso de Estudio de Comunicaciones Seguras sobre Redes Móviles AD HOC nos expone aspectos a tener en cuenta para la elección del nivel de seguridad teniendo en cuenta el equilibrio entre seguridad y consumo de recursos:

- Utilizar el protocolo HTTP en lugar de FTP
- Utilizar OpenVPN con compresión LZO, siempre y cuando la relación de compresión sea superior al 30%.
- Si se va utilizar solamente HTTP y lo que se busca optimizar el rendimiento la opción a elegir es HTTPS.
- Si se va utilizar solamente HTTP y se busca un menor consumo de energía la mejor opción es HTTP sobre OpenVPN o L2TP/IPSEC.
- Si además de HTTP se van a utilizar otros protocolos que requieran transporte TCP y cuando la prioridad sea el rendimiento (throughput, latencia y consumo de energía), la mejor alternativa es L2TP/IPSEC.
- El canal NO seguro es una opción a considerar cuando el ancho de banda y/o la energía sean muy limitados, ya que el uso de un canal seguro puede ocasionar que algunas aplicaciones dejen de funcionar correctamente por falta de ancho de banda o que la energía almacenada en la batería del nodo cliente se consuma muy rápidamente.

En el centro Nacional (en sus informes de ciberamenazas y tendencias) y ENISA (European Agency for Network and Information Security), año tras año se nota un incremento en el número de ataques y la sofisticación de estos, como se puede apreciar en la (Gráfico a). (Castro, Muñoz, Zhou, Informática, & Málaga, 2005)

Gráfico a. Evolución de incidencias gestionados por el CCN-CERT

Fuente: Sistemas Embebidos en Red Seguros (2017)

JUSTIFICACIÓN

Justificación Teórica

En la actualidad este sistema de red de sensores inalámbricos ha llegado a incrementarse notablemente en los diferentes ámbitos como la observación y soluciones integrales para la monitorización, detección y el pronóstico de riesgos y eventos meteorológicos, convirtiéndose en una herramienta importante al ofrecer una alerta temprana, y disminuir el impacto que puede provocar. Sin embargo, esta red al poseer una gran cantidad de nodos requiere de mayor consumo de energía la cual puede verse afectada por los principales factores que varíen el rendimiento de la red.

Estos sensores no cuentan con gran capacidad de memoria, de manera que la información que se puede enviar es limitada y el tratar de colocar un algoritmo que brinde un alto grado de seguridad no es posible, ya que necesitaría de recursos con los cuales no cuenta; por lo tanto, se necesita realizar un análisis de un algoritmo que cuente con un grado satisfactorio de seguridad sin comprometer la energía que ocupa el sensor ni restringir la memoria que posee.

Se ha visto que las redes WSN son vulnerables a ataques de seguridad y al tener limitaciones en su capacidad, se deben proporcionar servicios mínimos de seguridad, los cuales pueden ser:

- Integridad de datos. Se debe asegurar mediante algún método que cualquier información que se haya recibido no haya sido modificada.
- Autenticación. Verificar que la información que se está recibiendo proviene de una fuente confiable.
- Confidencialidad de datos. Los nodos sensores deben crear un canal que asegure que la información y el envío de datos sean cifrados para protegerlos ante un ataque de análisis de tráfico.
- Protección física. El sistema debe tener mecanismos para evidenciar alteraciones físicas, así como proteger la información almacenada en la memoria física del dispositivo.

Justificación Aplicativa

Con el objetivo de dar mayor seguridad a la red de Monitoreo de Ondas Sísmicas con una topología en malla, enfocándonos en la confidencialidad y utilizando el estándar IEE 802.15.4 (Zigbee) para la comunicación entre los sensores, es necesario la inserción de un algoritmo de encriptación ya existente que pueda brindarnos la garantía de que la información transmitida por los sensores solo pueda ser visible por los entes idóneos, así como evitar que consuma demasiada energía por tener un nivel alto de robustez, sin que ningún nodo cese su funcionamiento por falta de alimentación. Para lograr esto, realizaremos una comparación de dos tipos algoritmos, estos fueron elegidos ya que presentan características que serán útiles en esta investigación, tales como el grado protección y bajo consumo energético.

Una vez hecha esta comparación, constatamos que tipo de encriptación (sea esta asimétrica o simétrica) nos brindará el equilibrio entre seguridad y consumo de energía para evitar, de este modo, que uno o más nodos queden inactivos, asegurando también el canal de transmisión. Para finalizar realizaremos una equiparación del consumo de energía antes de insertar el algoritmo y luego de hacerlo para obtener un porcentaje del aumento del consumo.

Este trabajo se realiza ya que se necesita encriptar este tipo de datos que son sensibles, para evitar que al ser capturados por un atacante este provoque falsas alarmas y esto a su vez conlleve pánico civil, gastos en evacuaciones y posibles accidentes a causa de la desesperación de la ciudadanía.

OBJETIVOS

Objetivo General

Evaluar la eficiencia energética en las comunicaciones encriptadas de una red de sensores inalámbricos (WSN) que monitorea ondas sísmicas

Objetivos Específicos

- Analizar los algoritmos de encriptación robustos que se pueden aplicar en una red WSN.
- Diseñar la Red que monitorice Ondas Sísmicas utilizando la topología de red en malla.
- Implementar un prototipo WSN que monitorice Ondas Sísmicas para evaluar la eficiencia energética
- Aplicar los algoritmos de encriptación en la red de estudio para establecer una comunicación segura.
- Verificar como se ve afectada la eficiencia energética al añadir un algoritmo de encriptación a la comunicación de la red implementada.

CAPÍTULO I

1 MARCO TEÓRICO

En este capítulo se describe las redes inalámbricas, se detallan varias características de las redes de sensores inalámbricas, así como un análisis comparativo de tecnologías inalámbricas presentes en estas redes. Por otro lado, se habla de los problemas de seguridad que presentan este tipo de comunicaciones.

1.1 Redes de Sensores Inalámbricas (WSN)

Las redes de sensores inalámbricos vienen definidas como redes auto configurado que no necesitan de una infraestructura fija, son utilizadas para el control de condiciones físicas o ambientales, tales como, movimiento, presión, sonido, temperatura, vibración o contaminante, para luego enviar toda esa información a una ubicación principal donde se observaran y analizaran cada uno de los datos obtenidos. (Alvaro, 2017)

Una estación base o receptor será el encargado de ser la interfaz entre el usuario y la red, de donde podremos recolectar la información en modo de consultas y así reunir los resultados que ha obtenido dicha red.

Una red de sensores contiene cientos de miles de nodos que se pueden comunicar entre ellos por medio de señales de radio, además cuentan con dispositivos de detección y computo, transceptores de radio y componentes de potencia para su funcionamiento autónomo. Un nodo sensor individual posee recursos restringidos tales como velocidad de procesamiento limitada, escasa capacidad de almacenamiento y ancho de banda de comunicación. (Architectural Based Data Aggregation, 2015,pag. 1131)

Al desplegar los nodos, estos son los responsables de auto organizar una infraestructura de red que sea apropiada que muy a menudo cuenta con comunicación de multisalto, como siguiente paso los sensores que se encuentran conectados inician con la recopilación de la información de interés.

Estos sensores al ser inalámbricos tienen la facilidad de realizar tareas a distancia como el envío de instrucciones específicas, como también proporcionar muestras de detección desde un sitio de control. Posee dos modos de funcionamiento, este puede ser continuo o al estímulo de algún evento, además con el sistema GPS y algoritmos de posicionamiento pueden obtener información de la ubicación de los sensores. (Architectural Based Data Aggregation, 2015,pag.1132)

Además de receptar y envía la información, estos sensores pueden ser equipados con actuadores que realicen alguna acción bajo ciertas condiciones.

Las redes inalámbricas de sensores (Ver Figura 1-1) permiten nuevas aplicaciones, pero requieren de protocolos que se adapten a las limitaciones de estos dispositivos como la poca complejidad del dispositivo y el bajo consumo de energía, ya que se busca que extender la vida útil de esta red obteniendo un equilibrio entre comunicación y capacidad de procesamiento de datos/señal.

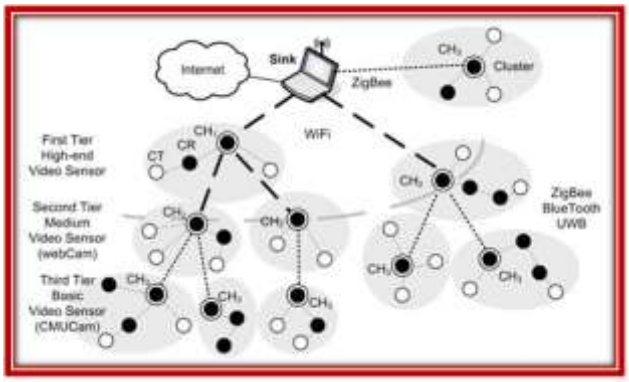

Figura 1-1. CERT Red Inalámbrica de Sensores

Fuente: http://omnet-manual.com/omnet-code-wsn/)

Características de una red de sensores

El desarrollo de las redes de sensores requiere tecnologías de tres áreas de investigación diferentes: detección, comunicación, y computación (incluyendo hardware, software y algoritmia).

Los nodos sensores se encuentran normalmente esparcidos en un campo sensor (Ver Figura 2-1). Cada uno de estos nodos sensores esparcidos por la red tiene capacidad tanto para recolectar datos, como para enrutarlos hacia el nodo recolector (sink node) mediante una arquitectura ad hoc de múltiples saltos. El nodo recolector puede comunicarse con el nodo administrador (gestor de tareas) vía Internet, vía satélite o de forma directa. (Matin, et al, 2012,pag. 2)

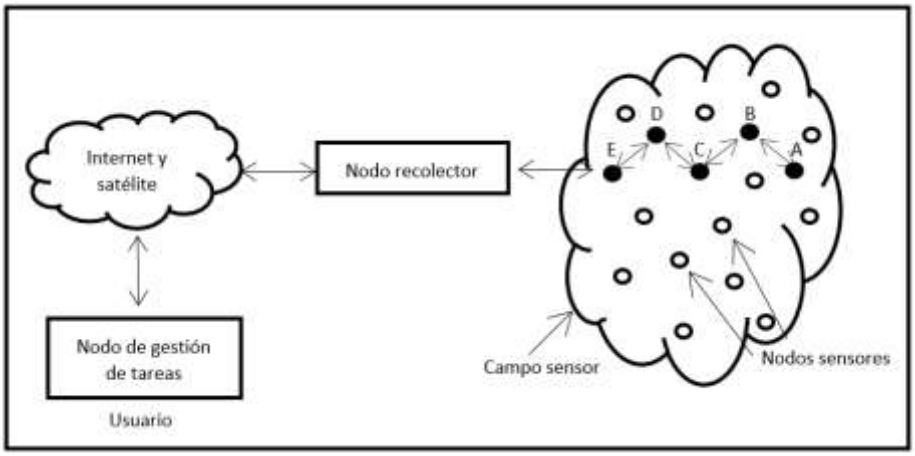

Figura 2-1. Estructura de una Red de Sensores

Realizado por: Andrés Solís, Ítalo Parreño, 2019

El diseño de una red de sensores como la descrita aquí está altamente influenciado por los siguientes factores:

- Tolerancia a fallos: Algunos nodos sensores pueden fallar o bloquearse debido a la falta de energía, o recibir daños físicos o interferencias medioambientales. El fallo de nodos sensores no debería comprometer el funcionamiento global de la red sensora. Este es el principio de la tolerancia a fallos o fiabilidad. (Arano, 2010)

- Escalabilidad: Los nuevos diseños deben ser capaces de trabajar con un número de nodos del orden de centenares, millares, e incluso, dependiendo de la aplicación, millones. También deben tener en cuenta la alta densidad, que puede llegar hasta algunos centenares de nodos sensores en una región, que puede ser menor de 10 metros de diámetro. (Arano, 2010)

- Costes de producción: Dado que las redes de sensores consisten en un gran número de nodos sensores, el coste de un nodo individual es clave para que una red inalámbrica sea rentable en comparación con una cableada. Si el coste de la red es más caro que el despliegue de sensores tradicionales, la red sensora no está justificada desde el punto de vista económico. (Arano, 2010)

- Limitaciones hardware: Un nodo sensor está constituido por cuatro componentes básicos, como muestra la Figura 3-1 Estructura de un sensor: una unidad sensora, una unidad de proceso, una unidad transceptora, y una unidad de energía, aunque pueden tener también

componentes adicionales dependiendo de su aplicación como un sistema de localización, un generador de energía o un movilizador. (Matin, et al, 2012,pag. 4)

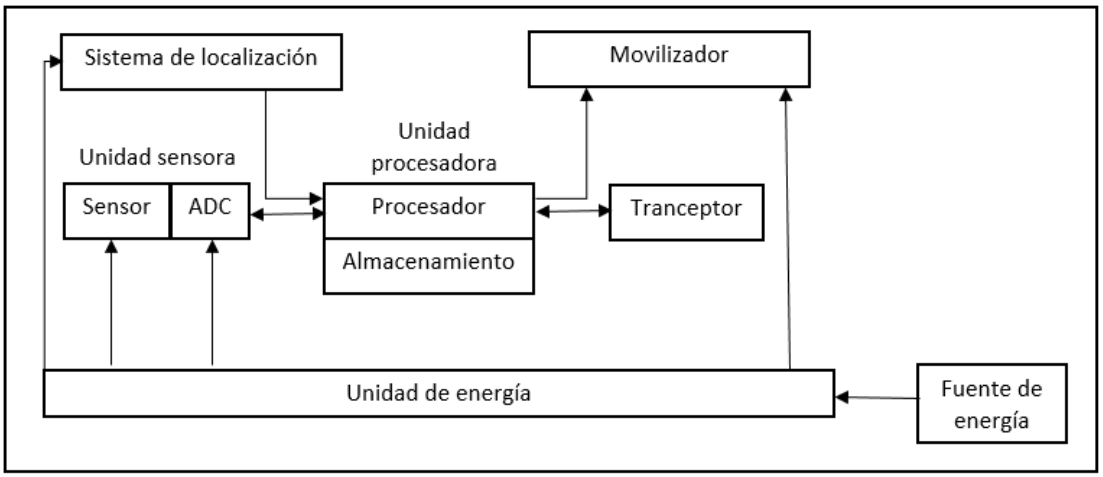

Figura 3-1. Estructura de un Sensor

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Las señales analógicas producidas por los sensores, basadas obviamente en el fenómeno observado, son convertidas a señales digitales por el conversor ADC, para ser pasadas después a la unidad de proceso. La unidad de proceso, generalmente asociada a una pequeña unidad de almacenamiento, maneja los procedimientos necesarios para que el nodo sensor colabore con los demás en la realización de las tareas de percepción asignadas. (Matin, et al, 2012,pag. 5)

Uno de los componentes más importantes de un nodo sensor es la fuente de alimentación. La fuente de alimentación puede ser abastecida por unidades captadoras de energía como es el caso de las células solares.

El despliegue de un gran número de nodos densamente distribuidos precisa de un mantenimiento y gestión de la topología cuidadosos. Se pueden dividir las tareas de mantenimiento y cambio de la topología en tres fases:

- Pre-despliegue y despliegue: Los nodos sensores pueden ser arrojados en masa o colocados uno por uno en el campo sensor.
- Post-despliegue: Después del despliegue, los cambios de topología son debidos a cambios en la posición de los nodos sensores, accesibilidad (debido a interferencias intencionadas (jamming), ruido, obstáculos móviles, etc), energía disponible, funcionamiento defectuoso y detalles de las tareas encomendadas.

- Despliegue de nodos adicionales: Nodos sensores adicionales pueden ser desplegados en cualquier momento para reemplazar nodos defectuosos o debido a cambios en la dinámica de las tareas.

Los nodos sensores son desplegados densamente bien muy cerca o directamente en el interior del fenómeno a ser observado. Por consiguiente, normalmente trabajan desatendidos en áreas geográficas remotas. Pueden estar trabajando en el interior de maquinaria grande, en el fondo del océano, en un área contaminada biológicamente o químicamente, en un campo de batalla más allá de las líneas enemigas, así como en edificios y hogares.

En una red de sensores multisalto, los nodos de comunicaciones están conectados mediante un medio inalámbrico. Estas conexiones pueden estar formadas por medios radio, infrarrojo o óptico, aunque la gran mayoría del hardware actual para redes de sensores está basada en RF.

Otro posible modo de comunicación entre nodos en redes de sensores es mediante infrarrojos. La comunicación por infrarrojos no necesita licencia y es robusta frente a interferencias producidas por dispositivos eléctricos. Los transceptores basados en infrarrojos son baratos y fáciles de construir. Otro desarrollo interesante es el del Smart Dust, que es un sistema autónomo de percepción, computación y comunicación que utiliza el medio óptico para transmitir. Ambos medios, infrarrojos y ópticos, requieren de visión directa entre el nodo o nodos transmisores y receptores.

- **Consumo energético**: Los nodos sensores inalámbricos, por lo general, están equipados con una fuente energética limitada (< 0,5 Ah, 1.2 V). En los escenarios de algunas aplicaciones, la recarga de los recursos energéticos puede ser imposible. El tiempo de vida de los nodos sensores, en consecuencia, muestra una gran dependencia del tiempo de vida de la batería.

  En una red sensores ad hoc multisalto, cada nodo desempeña el doble rol de origen de información y enrutador de información. El funcionamiento defectuoso de algunos nodos puede causar cambios de topología significativos y puede requerir re-enrutamiento de los paquetes y reorganización de la red. De aquí que, la conservación y administración energética tomen una importancia adicional.

- **Elementos de una WSN**

  Una Red de Sensores Inalámbrica está formada por varios elementos, para que los elementos en conjunto puedan lograr el funcionamiento normal de la WSN y cumplir con la transmisión de la información que la red está programada a realizar, existen elementos principales, sirven de base para el funcionamiento de una Red de Sensores Inalámbrica los cuales son: Nodos Sensoriales (Motas), Nodos Coordinadores, *Gateway*, Estación Base. (Ver Figura 4-1)

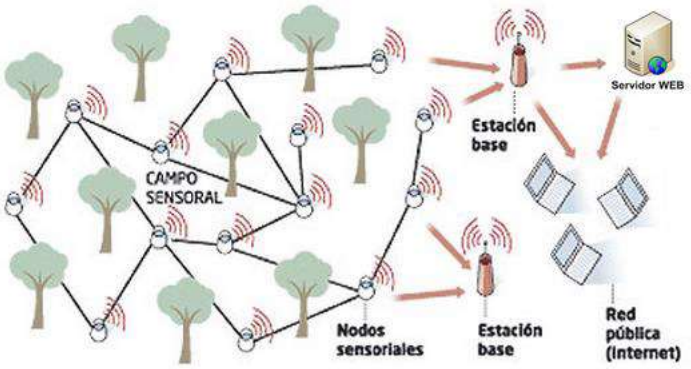

Figura 4-1. Elementos de la Red WSN

Fuente: https://www.researchgate.net/figure/Figura-1-Elementos-principales-de-una- WSN_fig1_297208802

- **Nodos Sensoriales (Motas):** Los Nodos Sensoriales también conocidos como Motas son elementos de la WSN que se encargan de la recolección de información mediante sensores de algún evento o fenómeno físico. Se encuentran construidos mediante un módulo de Sensores, un módulo de procesamiento y un módulo de transmisión inalámbrica, todo esto alimentado por una fuente de energía independiente,

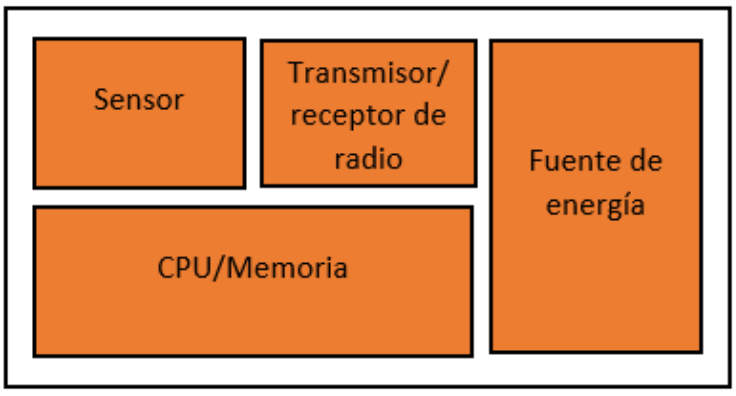

Figura 5-1. Componentes del Nodo

Fuente: Andrés Solís, Ítalo Parreño, 2019

Los nodos sensoriales están diseñados en placas (Ver Figura 5-1), las cuales incluyen módulos como: los sensores, el circuito micro controlador encargado del procesamiento, la interfaz de transmisión inalámbrica y la fuente de energía (batería de corriente continua (CC), o un conjunto de baterías pequeñas). En general un Nodo Sensorial suele tener un tamaño de dimensiones pequeñas, cada nodo sensorial es programado para enviar la información que obtiene hacia un nodo en específico o hacia un conjunto de nodos de la red.

- **Nodos Coordinadores:** son los nodos encargados de recibir toda la información enviada por cada nodo sensorial dentro de la WSN, cada nodo coordinador recibe la información de la WSN de manera inalámbrica, agrupando esta información y reenviándola hacia el equipo encargado del almacenamiento o tratamiento de la información que puede ser a manera de ejemplo un servidor de datos.
- **Gateway:** es el elemento encargado de interconectar la Red de Sensores Inalámbrica con una red TCP/IP, este elemento permite que toda la información recopilada dentro de la WSN se pueda enviar hacia redes de datos Ethernet y con esto la salida de la información hacia internet.
- **Estación Base:** es donde se recibe toda la información de la red para su procesamiento y entendimiento, en la estación base se encuentran concentrados tanto los nodos coordinadores, los equipos que almacenan información (computadores) y los *gateways*, de esta manera en la estación base se encuentran los equipos que permiten procesar la información de la WSN para la visualización de la misma.

1.1.1 Arquitecturas

1.1.1.1 Arquitectura Centralizada

Esta es la arquitectura más simple de las redes de sensores inalámbricos (Ver Figura 6-1), en la cual podemos aplicar el proceso de fusión de datos, cuyo proceso es cada nodo sensor que detecta el dato lo trasmite al su único nodo central denominado nodo de fusión del procesador central, que se encarga de fusionar los informes recopilado por todos los nodos. La responsabilidad de toda la red recae en el nodo central.

La ventaja de esta arquitectura es la fácil detección de algún informe erróneo que haya sido enviado por esta red de sensores. Por otro lado, la desventaja que presenta es que es inflexible a los cambios de los sensores y la carga de trabajo está reunida en un solo punto. (Architectural Based Data Aggregation, 2015,pag.1133)

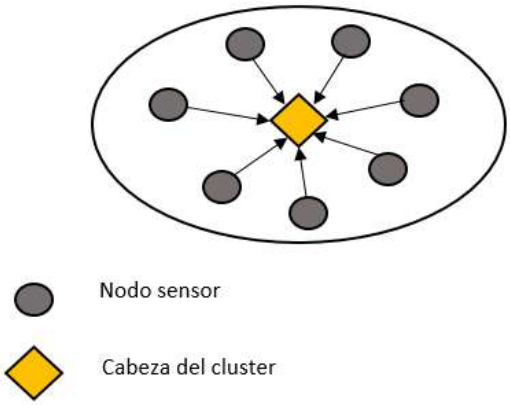

Figura 6-1. Arquitectura centralizada WSN

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.1.2 Arquitectura Descentralizada

A diferencia de la anterior, en esta arquitectura no existe un solo nodo encargado de tomar las decisiones, cada uno de los miembros de la red (nodos) posee el proceso de fusión de datos, teniendo acceso a la base de observaciones y obtener la información de los nodos vecinos puesto que todos nos nodos se encuentran conectados entre sí.

La ventaja de la arquitectura descentralizada es la escalabilidad y tolerancia frente a la adición o pérdida de los nodos así también a los cambios dinámicos que puede tener la red. (Ver Figura 7-1) (Architectural Based Data Aggregation, 2015,pag.1133)

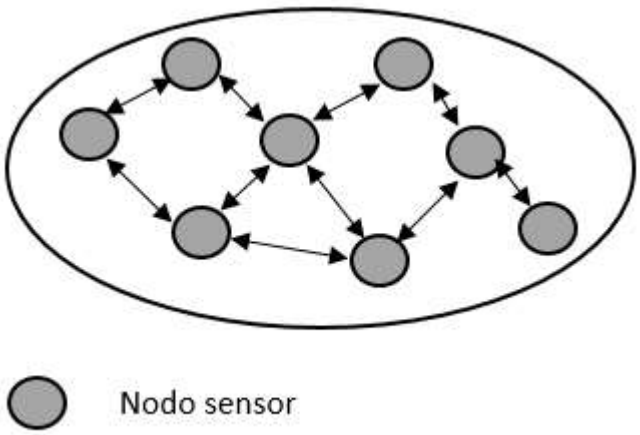

Figura 7-1. Arquitectura Descentralizada

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.1.3 Arquitectura Jerárquica

En esta arquitectura todos los nodos que conforma la red se encuentran divididos en niveles jerárquicos (Ver Figura 8-1), el nivel 0 consta de los sensores normales distribuidos en un área topográfica que, para minimizar la potencia de trasmisión, los nodos sensores envían los datos a los nodos de fusión mediante un algoritmo de enrutamiento que permita disminuir el consumo de potencia.

Los datos del sensor pueden enviarse al nodo de fusión más cercano utilizando dos técnicas de enrutamiento las cuales son: difusión directa o inundación simple.

La ventaja que posee es el balanceo de carga equilibrado entre los nodos que conforman esta red. (Architectural Based Data Aggregation, 2015,pag.1134)

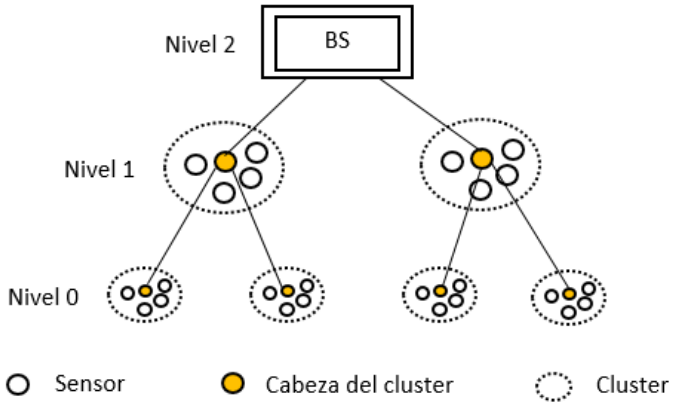

Figura 8-1. Arquitectura Jerárquica

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.2 Tipos de Redes WSN

1.1.2.1 Terrestrial WSN

Este tipo de red consiste en una gran cantidad de nodos de bajo costo que se encuentran distribuidos en un área determinada desplegados en la tierra generalmente de manera ad-hoc (colocados mediante un avión que los arroja a la tierra) (Ver Figura 9-1), estos nodos deben ser capaces de enviar la información obtenida a la estación base de manera efectiva en un entorno denso.

Dado que estos nodos cuentan un con fuente de energía limitada que en la mayoría de los casos no es recargable, normalmente se los equipa con una fuente secundaria de alimentación, como por ejemplo una celda solar, a su vez la energía de la batería se puede conservar realizando un enrutamiento optimo, con un corto rango de transmisión, la agregación de datos dentro de la red y el uso de operaciones de un ciclo bajo de trabajo.

Las aplicaciones que se destacan con este tipo de red de sensores es la detección y monitoreo ambiental, las exploraciones de la superficie, como también el monitoreo industrial. (Wireless Sensor Networks: recent developments and, 2013,pag. 7)

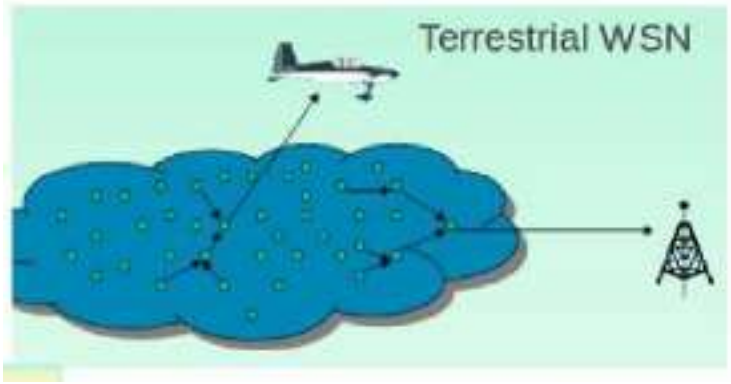

Figura 9-1. WSN terrestre

Fuente: K. Berberidis, D. Ampeliotis, 2013, pag. 7

1.1.2.2 Underground WSN

En una red inalámbrica de sensores subterránea, los nodos que conforman la misma se encuentran situados en cuevas, minas o debajo de la tierra con la finalidad de monitorear las condiciones subterráneas (Ver Figura 10-1). Para lograr transmitir la información de los nodos subterráneos, son conectados a otros nodos que se sitúan por encima del nivel del suelo.

El costo de este tipo de red es más elevado que los WSN terrestres, ya que se necesita garantizar una comunicación integra a través del suelo, las rocas o cualquier superficie.

Otro problema de esta red es la comunicación inalámbrica ya que al estar por debajo de la superficie la atenuación de la señal aumenta y pueden existir pérdidas considerables, sin contar que el trabajo de reemplazo de baterías de los nodos que se encuentran enterrados se vuelve una tarea complicada, por lo que es indispensable el diseño de una comunicación eficiente que ayude a disminuir el consumo energético para prolongar la vida útil de la red.

Las WSN subterráneas son utilizadas en una gran variedad de aplicaciones, estas pueden ser: supervisión de agricultura, control de la frontera militar, monitorización subterránea del suelo, agua o minerales que lo conforman y la gestión del paisaje. (Wireless Sensor Networks: recent developments and, 2013,pag. 7)

Figura 10-1. WSN subterránea

Fuente: K. Berberidis, D. Ampeliotis, 2013, pag 7.

1.1.2.3 Underwater WSN

Los sensores de este tipo de red se encuentran desplegados bajo el agua (cualquier medio marino), al ser elevado el costo de los mismos, se implantan en una pequeña cantidad y se utilizan vehículos submarinos autónomos que tienen la tarea de explorar y recopilar la información de los nodos. (Ver Figura 11-1)

La comunicación inalámbrica que presenta este tipo de red hace que sea un desafío en la implementación, ya que, al utilizar ondas acústicas, estas poseen un ancho de banda limitado, un largo retardo en la propagación, alta latencia y muchos problemas en el desvanecimiento de la señal. Por lo que estos nodos deben ser capaces de adaptarse a condiciones extremas del ambiente oceánico y lograr auto configurarse para un correcto funcionamiento.

Por otro lado, como se comentó anteriormente los nodos poseen una cantidad limitada de energía que no se puede reemplazar ni recargarse, esto hace que la comunicación submarina tiene que ser eficiente y las técnicas de conexión de la red deben ser fiables.

Entre las aplicaciones más utilizadas de este tipo de red están el monitoreo de la contaminación, exploración y vigilancia submarina, monitorización sísmica, monitoreo y prevención de desastres, monitoreo de equipos y robótica subacuática entre otros. (Wireless Sensor Networks: recent developments and, 2013,pag. 8)

Figura 11-1. WSN subacuática

Fuente: K. Berberidis, D. Ampeliotis, 2013, pag. 8.

1.1.2.4 Multimedia WSN

Consiste en nodos sensores de bajo coste equipados con cámaras y micrófonos, desplegados de forma preestablecida para garantizar la cobertura. Los dispositivos de sensores multimedia son capaces de almacenar, procesar y recuperar datos multimedia como vídeo, audio e imágenes. Deben hacer frente a diversos retos, como la elevada demanda de ancho de banda, el elevado consumo de energía, el suministro de calidad de servicio (QoS), el procesamiento y la compresión de datos y el diseño de capas cruzadas.

Es necesario desarrollar técnicas de transmisión que soporten un alto ancho de banda y un bajo consumo de energía para entregar contenidos multimedia como un flujo de vídeo. Aunque el aprovisionamiento de QoS es difícil en las redes WSN multimedios debido a la capacidad de enlace variable y al retardo, debe alcanzarse un cierto nivel de QoS para una entrega de contenido fiable. (Wireless Sensor Networks: recent developments and, 2013,pag. 8)

1.1.2.5 Mobile WSN

Consiste en nodos sensores móviles que pueden moverse e interactuar con el entorno físico. Los nodos móviles pueden reposicionarse y organizarse en la red además de ser capaces de sentir, calcular y comunicarse. Un algoritmo de enrutamiento dinámico debe, por lo tanto, ser empleado como un enrutamiento fijo en WSN estático.

Las WSN móviles se enfrentan a diversos retos, tales como el despliegue, la gestión de la movilidad, la localización con movilidad, la navegación y el control de los nodos móviles, el mantenimiento de una cobertura de detección adecuada, la minimización del consumo de energía en la locomoción, el mantenimiento de la conectividad de la red y la distribución de datos.

Los principales ejemplos de aplicaciones móviles de la WSN son el monitoreo (medio ambiente, hábitat, submarino), la vigilancia militar, el rastreo de objetivos, la búsqueda y el rescate. Se puede lograr un mayor grado de cobertura y conectividad con los nodos de sensores móviles en comparación con los nodos estáticos. (Wireless Sensor Networks: recent developments and, 2013,pag, 8)

1.1.3 Topologías

La tecnología descrita permite configurar en topologías como: estrella, árbol y malla. Para ello se necesitan: dispositivos finales, motas y un *Gateway*, se debe tener en cuenta que algunos dispositivos pueden cumplir varios roles ya que depende mucho de su configuración.

1.1.3.1 Topología Estrella

Este tipo de topología consta de una única estación base la cual puede enviar, así como también recibir mensajes a un número de nodos remotos, estos últimos solo pueden enviar o recibir mensajes a la estación base de modo que no se pueden comunicar entre nodos. (Ver Figura 12-1) (Matin, et al, 2012,pag. 5)

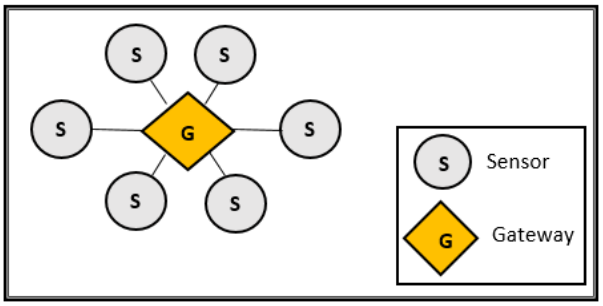

Figura 12-1. Topología en Estrella

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 1-1, se puede observar las principales ventajas y desventajas que tiene la topología descrita anteriormente.

Tabla 1-1. Ventajas y Desventajas de la Topología en Estrella

Ventajas	**Desventajas**
Poca latencia	No siempre es posible desarrollar
La red es más sencilla	Escalabilidad baja
Gasto de energía de forma igual	Problemas de colisión con el aumento de nodos coordinadores
Fácil de implementación	Si existe falla del nodo central se daña la red
Topología muy resistente	

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.3.2 Topología en Malla

Una red de malla (Ver Figura 13-1) permite transmitir datos de un nodo a otro nodo de la red que está dentro de su rango de transmisión de radio. Se conoce como multi-hop, es decir, si un nodo quiere enviar un mensaje a otro nodo que está fuera de su rango de radiocomunicaciones, puede utilizar un nodo intermedio para reenviar el mensaje al nodo deseado. (Moya, 2016)

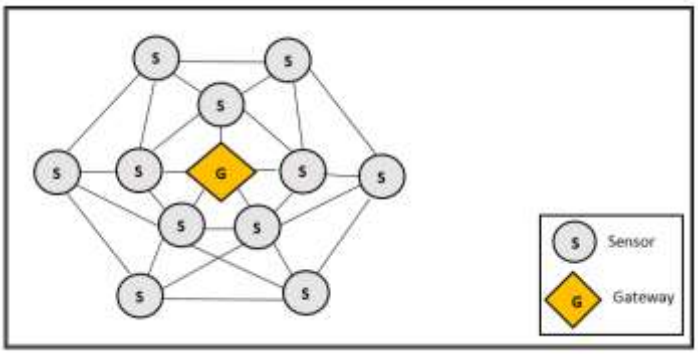

Figura 13-1. Topología en Malla

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Si un nodo individual falla, un nodo remoto todavía puede comunicarse con cualquier otro nodo de su rango, que, a su vez, puede reenviar el mensaje a la ubicación deseada. A medida que aumenta el número de saltos de comunicación a un destino, el tiempo para entregar el mensaje también aumenta. (Matin, et al, 2012,pag. 6)

En la Tabla 2-1 se detalla las ventajas y desventajas de la topología en malla.

Tabla 2-1. Ventajas y Desventajas Topología en Malla

Ventajas	**Desventajas**
Menor costo	Alta complejidad del sistema
No necesita muchos Gateway para alcanzar una gran escalabilidad	Alta cantidad de colisiones
Transmisión de datos es continua aunque exista fallo de uno o varios nodos	Alta latencia en la red
En caso de fallo obtiene rutas alternas	Diferencias entre pruebas de laboratorio y desarrollo real
Se reduce el mantenimiento de los nodos	Tiene un desarrollo costoso
Son redes auto ruteables y auto configurables	
Es una red muy confiable	

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.3.3 Topología en Árbol

La conexión se realiza buscando el nodo de mayor jerarquía, es decir que los nodos miembros buscan al nodo coordinador y así sucesivamente hasta llegar al *Gateway*, en la cual los dispositivos se dividen como si de un árbol se tratase. (Moya, 2016)

Esta red utiliza un concentrador central denominado nodo raíz que es el encargado de enrutar las comunicaciones, jerárquicamente un hub central es el nivel a continuación del nodo raíz, que forma una red en estrella.

Esta red se puede considerar como la unión de topología en estrella y una de punto a punto, la ruta que puede elegir es de un solo salto o saltos múltiples, obteniendo los datos que detecta, enviándolos al receptor y este lo reenvía a su nodo principal todos los datos que se obtuvo de su propia red (red estrella).

Lo importante de la topología de red en árbol (Ver Figura 14-1) es encontrar la ruta más corta con un tiempo de vida máximo y un retraso más corto, pero aparece un problema en el balaceo de carga en cada nivel del árbol cuando existe una comunicación entre dos nodos. (Matin, et al, 2012,pag. 7)

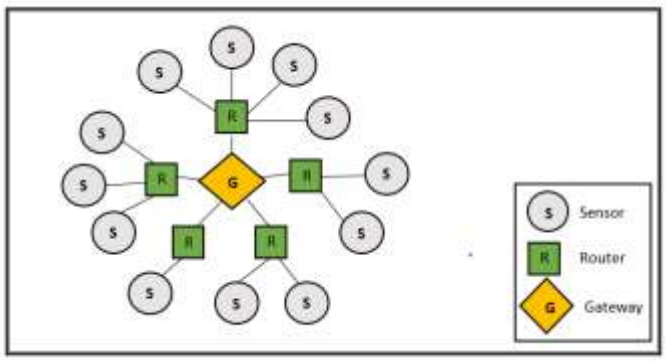

Figura 14-1. Topología en Árbol

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 3-1 podemos encontrar las ventajas y desventajas que presenta este tipo de topología.

Tabla 3-1. Ventajas y Desventajas Topología en Árbol

Ventajas	**Desventajas**
Las altas velocidades de topología de estrella es igual a esta topología	Puede llegar a ser costosas si se introducen router
Alta escalabilidad y bajo proporción de colisiones	Si un router falla puede caer una gran parte de la red
Es similar a la conexión utilizada de la topología de red de una Pc	Dificultad y costos altos al desarrollar un algoritmo de enrutamiento dinámico
	Poca confianza en los algoritmos de enrutamiento

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.4 Plataformas para desarrollo de Redes WSN

1.1.4.1 Arduino

Es una plataforma electrónica de código abierto que se basa en software y hardware muy fácil de usar (Ver Figura 15-1), esta plataforma es capaz de leer entradas como sensores, al presionar un botón o algún mensaje y transformarlos en una salida sea esta un motor, encender una luz o la activación de alguna alarma.

Gracias a que tiene un micro controlador se pueden enviar un conjunto de instrucciones para que las ejecute mediante el lenguaje de programación Arduino y con el software IDE que se basa en el procesamiento (Arduino).

Por a los beneficios que brinda, Arduino se ha convertido en cerebro de una gran infinidad de proyectos tanto sencillos como complejos, nacido como una herramienta para un prototipado rápido encaminado a estudiantes que no tienen mucho conocimiento en programación y electrónica, brinda acceso a muchos campos como aplicaciones IoT, impresión en 3D y entornos integrados. (Arduino)

Es compatible con los sistemas operativos Mac, Windows y Linux y puede ser utilizado por cualquier persona sean niños, aficionados o programadores, siguiendo las instrucciones que vienen en el kit o en línea en la comunidad de Arduino, a continuación, detallamos las ventajas que presenta utilizar Arduino:

- Económico

  En comparación con otras placas que contengan microcontroladores, arduino es relativamente más económico.
- Multiplataforma

  El IDE de arduino es compatible con varios sistemas operativos siendo estos Windows, Linux y Macintosh OSX ya que la mayoría están limitados a Windows.
- Entorno de programación sencillo y claro

  El software de Arduino es de fácil uso para principiantes, pero a su vez muy flexible para los usuarios más experimentados de manera que también puedan aprovecharlo (Arduino).

Figura 15-1. Arduino UNO

Fuente: R. Baxter, N. Hastings, A. Law, and E. J. . Glass, 2008, pp. 561–563

1.1.4.2 Waspmote

Es una plataforma de sensor inalámbrica de licencia abierta creada por Libelium que se especializa en el bajo consumo en nodos sensores permitiendo que estos se vuelvan completamente autónomos alimentados por solo una batería, de esta manera ofrece una vida útil que puede comprender desde 1 a 5 años obedeciendo al ciclo de trabajo y el radio con el que sea usado.

Esta idea comenzó ya que se querían crear una red de sensores inalámbricos, la división de código abierto de Libelium con la colaboración de Arduino diseñan el *Arduino XBee Shield*, con el cual pretendían concretar la idea, pero Arduino por sus limitaciones no cumplió con los requisitos necesarios (Libelium Comunicaciones Dsitribuidas SL).

Entre los problemas que surgieron era que no se podía apagar el regulador para obtener un modo de suspensión ya que si no se realizaba este descargaba tan rápido a la batería que se descargaría en pocos días o en el peor de los casos solo horas, otro inconveniente era la certificación de radio ya que los nodos debían implementarse en escenarios reales tales como fábricas, casas y ciudades enteras.

Por ende, se decidió crear un nuevo dispositivo que lograse trabajar con modos de bajo consumo y que la infraestructura sea completamente modular y de este modo se creó el *Waspmote* (Ver Figura 16-1), se aseguró que este dispositivo tenga compatibilidad con el IDE de Arduino permitiendo que la comunidad de este último pueda gozar de este nuevo equipo. (Libelium Comunicaciones Dsitribuidas SL).

Las Figura 17-1 nos permite conocer de manera más específica como se encuentran los pines distribuidos y la Figura 18-1 nos permite ver el Diagrama Esquemático del Microprocesador

que muestra del microprocesador que la tarjeta posee, permitiéndonos ver como cada pin va a conectado a una función en específico. (Libelium Comunicaciones Dsitribuidas SL)

Características Generales (Ver Tabla 4-1):

Tabla 4-1. Características Generales de Waspmote

Microcontrolador: ATmega1281	Frecuencia: 14.7456 MHz
SRAM: 8 kB	EEPROM: 4 kB
FLASH: 128 kB	SD card: 8 GB
Peso: 20 g	Dimensiones: 73.5 x 51 x 13 mm
Rango de Temperatura: [-30 ºC, +70 ºC]*	Reloj: RTC (32 kHz)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

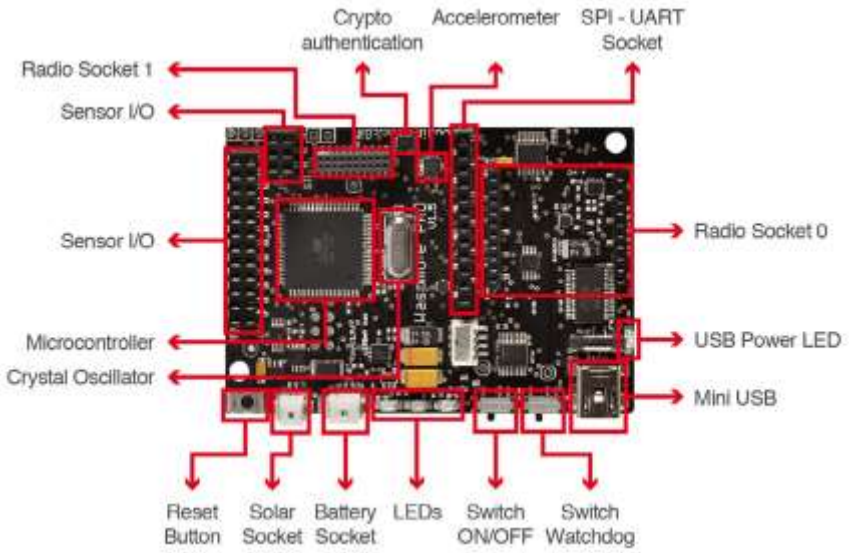

Figura 16-1. Waspmote

Fuente: Libelium Comunicaciones Distribuidas S.L., 2012, p 143.

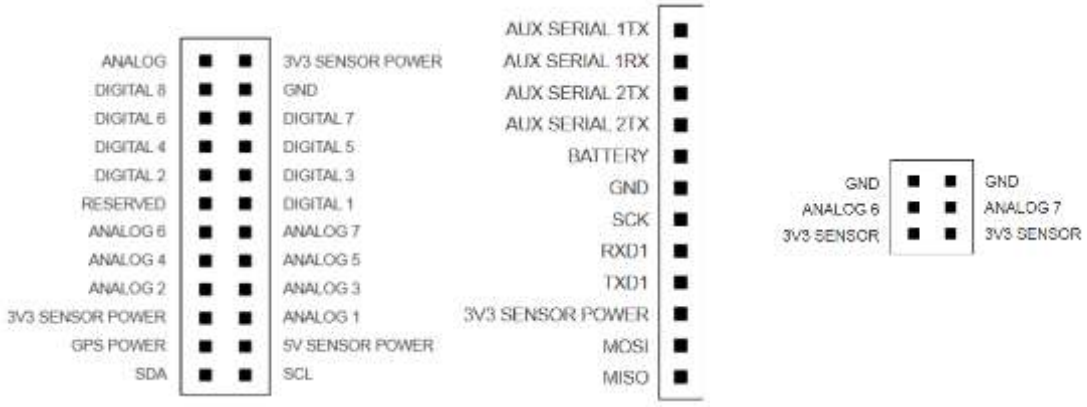

Figura 17-1. Descripción de los pines de los sensores

Fuente: Libelium Comunicaciones Distribuidas S.L. , 2012, p. 143.

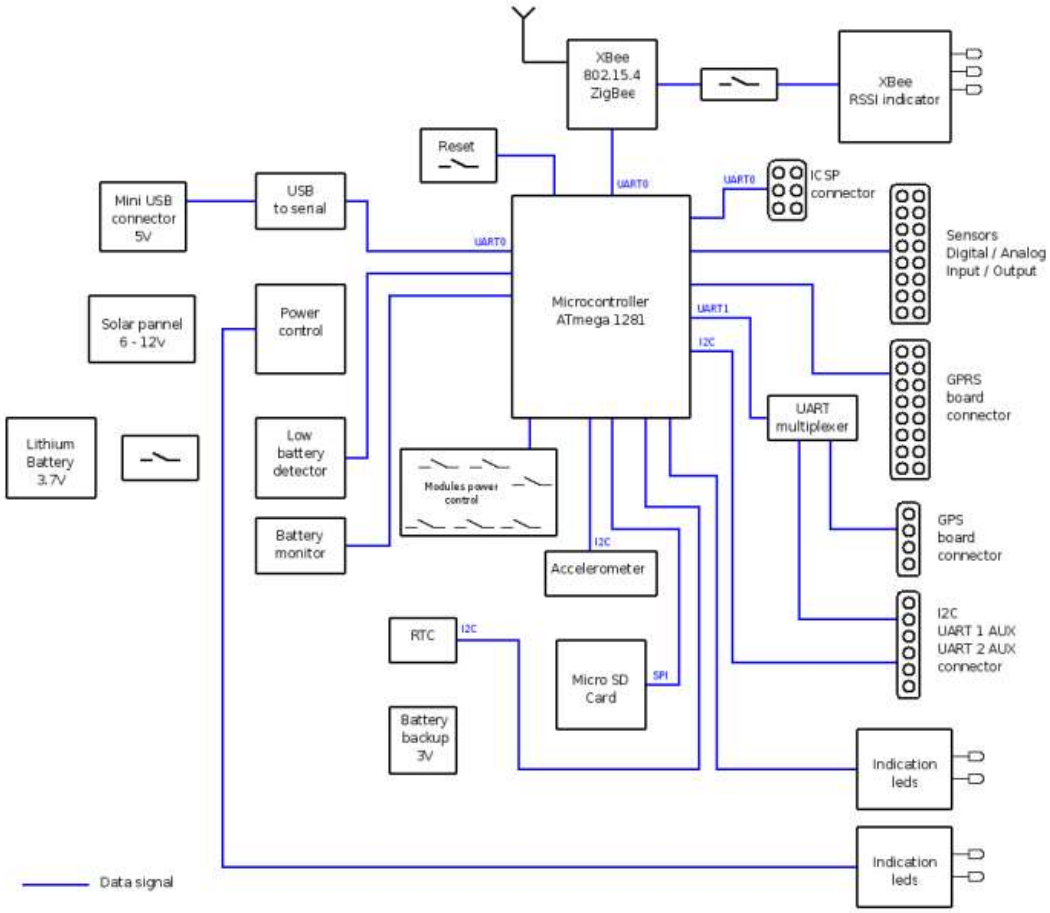

Figura 18-1. Diagrama de Bloques Waspmote

Fuente: Libelium Comunicaciones Distribuidas S.L,2012, .p. 143.

1.1.4.3 Raspberry

Se trata de una pequeña computadora no más grande que una tarjeta de crédito creada originalmente con fines educativos, nacido a partir de la idea de diseñar un dispositivo que mejore las habilidades de programación y comprensión de hardware con un muy bajo costo, pero poco a poco fue adoptado por fabricantes por su tamaño reducido y su bajo costo con la necesidad de implementar proyectos que requieran más de un micro controlador como ejemplo Arduino.

Aunque este dispositivo es más lento que una computadora de escritorio, se considera una computadora completa por las prestaciones que ofrece con la ventaja de un bajo consumo energético. Este dispositivo es de hardware abierto a excepción del chip principal el cual ejecuta la mayoría de componentes como el CPU, controladores USB, la memoria entre otros. (OpenSource)

El Raspberry-pi (Ver Figura 19-1) originalmente fue diseñado para el sistema operativo Linux y es así que casi todas las distribuciones de este poseen una versión optimizada para este dispositivo. Una ventaja del Raspberry es el tamaño de la comunidad que trabaja con esta pequeña computadora, si surge una pregunta sobre el proyecto que se esté realizando se podrá contar con una infinidad de personas dispuestas a contestar todas las dudas. (OpenSource)

Figura 19-1. Raspberry-pi

Fuente: Raspberry Pi Foundation, "Raspberry Pi 3 Model B," Datasheet, 2016.

En la Tabla 5-1 se detalla un Análisis Comparativo entre las tres plataformas con las cuales se pueden desarrollar redes WSN. Se encuentran las principales características que cada plataforma presenta.

Tabla 5-1. Análisis comparativo de Plataformas para Redes WSN

Dispositivo	Modelo	Dimensión	µc/CPU	Peso	I/O	SRAM	FLASH	Alimentación
Arduino	Mega	L: 10.2 cm A: 5.4 cm	ATmega2560	37 g	D: 54, A: 16	8 Kb	256 Kb	7-12V
Raspberry	3B	L:8.6 cm A: 5.7 cm	ARM Cortex-A53	45 g	HDMI,USB 2:4, ethernet, GPIO:40, MIPI:1	1 Gb	MicroSD slot	5V
Waspmote	V 1.2	L: 7.35 cm A: 5.1 cm	ATmega1281	20 g	D: 8, A: 7, UART: 2, I2C:1, SPI:1, USB:1	8 Kb	128 Kb	5V

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.5 Comparación de Tecnologías Inalámbricas para Redes WSN

- Bluetooth (IEEE 802.15.1)

Especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que permite la transmisión de datos y voz entre dos dispositivos por medio de una frecuencia (2.4 GHz), prescindiendo así de cables para su interconexión. Su uso resulta interesante cuando se tienen dos o más dispositivos en un área reducida sin grandes necesidades de ancho de banda. (Sempere, 2015) Existen 3 clases de Bluetooth en función de su alcance:

- Clase 1: 100 m aproximadamente.
- Clase 2: 10 m.
- Clase 3: 1 m.

- Wi-Fi (IEEE 802.11b)

Tiene una velocidad máxima de transmisión de 11 Mbps y emplea el mismo método de acceso definido en el estándar original CSMA/CA. Cabe destacar que a nivel práctico la velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbits sobre TCP y 7,1 Mbit/s sobre UDP, debido al espacio ocupado por la codificación de dicho protocolo.
Este estándar funciona en la banda de 2,4 GHz y se deben conectar preferentemente utilizando el estándar 802.11g, dando lugar a Wi-Fi (802.11b/g). Esto sirve para evitar la degradación de las celdas al utilizar los mecanismos de seguridad en toda la red inalámbrica. (Sempere, 2015)

- ZigBee (IEEE 802.15.4)

En este estándar se definen los niveles de red básicos para dar servicio a un tipo específico de red WPAN centrada en la habilitación de comunicación entre dispositivos ubicuos con baja complejidad, pequeño consumo de energía, conectividad inalámbrica de baja velocidad de datos entre dispositivos (a diferencia de estándares más orientados directamente a los usuarios medios, como Wi-Fi) y de bajo coste. (Garbarino, 2011)

La tasa de datos bruta debe ser lo suficientemente alta (200 kbps como máximo) para satisfacer un conjunto de necesidades simples, siendo adaptable a las necesidades de censado y automatización para comunicaciones inalámbricas (10 kbps o menos).

Se enfatiza el bajo coste de comunicación entre nodos cercanos (con o sin infraestructura) para favorecer aún más el bajo consumo. En la Tabla 6-1 se muestra una comparativa entre las tecnologías inalámbricas descritas anteriormente:

Tabla 6-1. Análisis Comparativo entre Tecnologías

Comparación entre Tecnologías Inalámbricas			
	WiFi (IEEE 802.11g)	**Bluetooth (IEEE 802.15.1)**	**ZigBee (802.15.4)**
Radio	DSSS (Direct Sequence Spread Spectrum)	FHSS (Frequency Hopping S (Garbarino, 2011)pread Spectrum)	DSSS (Direct Sequence Spread Spectrum)
Velocidad	54 Mbps	1 Mbps	250 kbps
Número de Nodos por Máster	32	7	64000
Latencia	Up to 3 s	Up to 10 s	30 ms
Tipos de Datos	Video,audio,gráficos,película, ficheros	Audio,gráficos,películas, ficheros	Pequeños paquetes de datos
Alcance (m)	100	10 (v1.1)	70 – 100
Expansión	Roamming	No	Si
Duración de la Batería	12 y 48 horas	1 semana	100 - 1000 días
Complejidad	Complejo	Muy complejo	Sencillo
Aplicación Principal	WLAN Corporativa	WPAN	Control y Monitorización
Memoria necesaria	1 MB+	250 KB+	4 KB - 32 KB
Parámetros más importantes	Velocidad y flexibilidad	Costes y perfiles de aplicación	Fiabilidad, bajo consumo y bajo coste

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.6 Sensores

Se trata de un dispositivo eléctrico o mecánico que transforma magnitudes físicas como la luz, la presión, el nivel del agua, etc., en valores que se puedan describir con un valor numérico y los cuales podemos manipular, estos valores son enviados a una placa recolectora o a su vez a un micro controlador que iniciará algún proceso o interactuará con otras variables dentro del mismo, este proceso tiene tres etapas descritas a continuación:

- El sensor capta el fenómeno físico y lo traduce a una señal eléctrica que dependerá de la variable física medida.
- La señal que emite el sensor es convertida por medio de un acondicionamiento dando como resultado un voltaje a su salida.
- La tensión obtenida del paso anterior entra a un conversor de A/D, el cual transforma de una tensión continua a la señal discreta.

1.1.6.1 Sensor de Vibración MEAS

El sensor de la lengüeta de la vibración de la película piezoeléctrica consiste en una película piezoeléctrica flexible laminada a un substrato del polímero. (Ver Figura 20-1)

Figura 20-1. Sensor de Vibración MEAS

Fuente: Msi, "Tech manual - Piezo Film Sensors,"

- PROPIEDADES DE LA PELÍCULA PIEZOELÉCTRICA

La película piezoeléctrica es un plástico de ingeniería flexible, ligera y resistente disponible en una amplia variedad de materiales. Espesores y grandes superficies. Sus propiedades como transductor incluyen:

- Amplio rango de frecuencia de 0,001 Hz a 109 Hz.
- Amplio rango dinámico (10-8 a 106 psi o: torr a Mbar).
- La baja impedancia acústica se ajusta a los sistemas de agua, tejido humano y adhesivos.
- Alta elasticidad

-Salida de alta tensión: 10 veces más alta que la de la cerámica piezoeléctrica para la misma entrada de fuerza.

-Alta rigidez dieléctrica: soporta campos fuertes (75V/:m) en los que la mayoría de las cerámicas piezoeléctricas despolarizar.

-Alta resistencia mecánica y al impacto (módulo 109-1010 Pascal)

-Alta resistencia a la humedad (<0.02% de absorción de humedad), la mayoría de los productos químicos, oxidantes, e intensa radiación ultravioleta y nuclear.

-Puede ser fabricado en diseños inusuales.

-Se puede pegar con adhesivos comerciales.

Una de las principales ventajas de la película piezoeléctrica sobre la cerámica piezoeléctrica es su baja impedancia acústica, que está más cerca a la del agua, el tejido humano y otras materias orgánicas. (Parallax)

Por ejemplo, la impedancia acústica (ZO = D L) de la película piezoeléctrica es sólo 2,6 veces mayor que la del agua, mientras que la de la cerámica piezoeléctrica suele ser 11 veces mayor. Una coincidencia de impedancia cercana permite una transducción más eficiente de las señales acústicas en el agua. y tejido. (Parallax)

La película piezoeléctrica tiene algunas limitaciones para ciertas aplicaciones. Esto hace que un transmisor electromecánico en comparación con la cerámica, especialmente en resonancia y en baja temperatura. Aplicaciones de frecuencia. La película de copo limero tiene temperaturas máximas de operación/almacenamiento tan altas como 135oC, mientras que el PVDF no se recomienda para uso o almacenamiento por encima de 100 EC. Además, si los electrodos de la película están expuestos, el sensor puede ser sensible a la radiación electromagnética. Buen apantallamiento está disponible para entornos de EMI/RFI de alto nivel. (Msi, 2008)

La película piezoeléctrica tiene baja densidad y excelente sensibilidad, y es mecánicamente resistente. El cumplimiento de es 10 veces mayor que la conformidad de la cerámica. Cuando se extrude en una película delgada, los polímeros piezoeléctricos pueden fijarse directamente a una estructura sin perturbar su funcionamiento mecánico movimiento. La película piezoeléctrica es muy adecuada para aplicaciones de detección de deformaciones que requieren un ancho de banda muy amplio y alta sensibilidad. Como actuador, la baja impedancia acústica del polímero permite una transferencia eficiente de una banda ancha de energía en aire y otros gases. (Msi, 2008)

- PROPIEDADES DE FUNCIONAMIENTO DE UN ELEMENTO DE PELÍCULA PIEZOELÉCTRICA TÍPICO

El elemento DT1 es una configuración de película piezoeléctrica estándar que consiste en un área activa de 12x30 mm. Impreso con electrodos de tinta de plata en ambas superficies de un sustrato de polímero piezoeléctrico troquelado de 15x40 mm.

1. Conversión electromecánica
   (3 dirección) 23 x 10-12m/V, 700 x 10-6N/V
   (3 direcciones) -33 x 10-12m/V

2. Conversión Mecánico-Eléctrica
   (1 dirección) 12 x 10-3V por micro deformación, 400 x 10-3V/:m, 14,4V/N
   (3 direcciones) 13 x 10-3V/N

3. Conversión piro eléctrica
   8V/ o K (@ 25 o C)

4. Capacitancia
   1.36 x 10-9F; Factor de disipación de 0.018 @ 10 KHz; Impedancia de 12 KS @ 10 KHz

5. Voltaje máximo de operación
   DC: 280 V (produce un desplazamiento de 7:m en una dirección)
   AC: 840 V (rinde 21: m de desplazamiento en 1 dirección)

6. Fuerza máxima aplicada (en la rotura, 1 dirección)
   6-9 kgF (produce una salida de tensión de 830 a 1275 V)

1.1.7 Software utilizado

1.1.7.1 Waspmote IDE

Este software es el kit de desarrollo de *Waspmote*, es usado para escribir y cargar los códigos en esta plataforma, además de monitorear la salida serial y la depuración del código. Gracias a que se creó en base a que sea compatible con Arduino, se pueden utilizar programas hechos con este último con pequeñas modificaciones. (Página libelium)

Es un programa de licencia libre lo que nos permite manipularlo en su totalidad sin la necesidad de una licencia de paga, la versión con la que trabajamos es la v06.05, en la Figura 21-1 se observa la ventana de trabaja de Waspmote IDE.

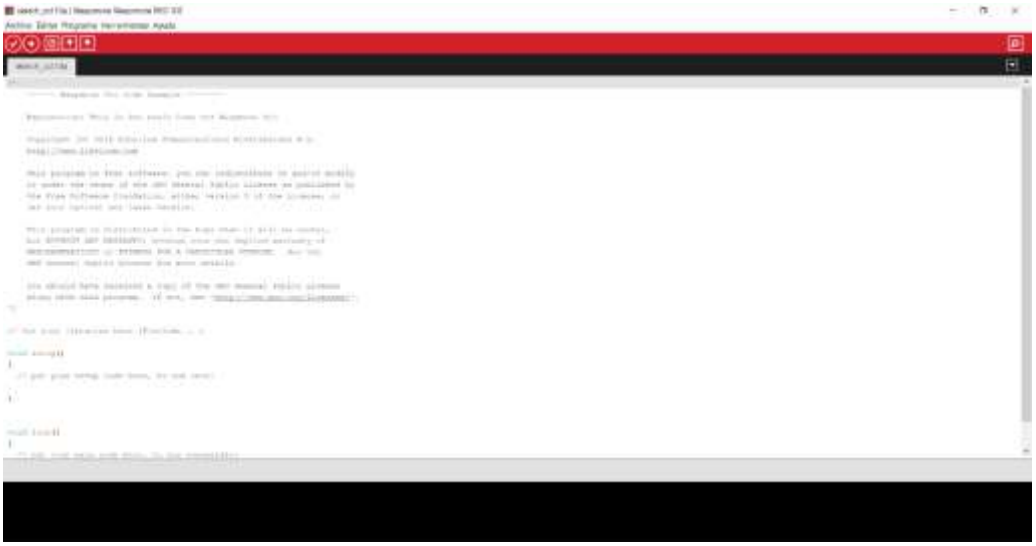

Figura 21-1. Entorno gráfico Waspmote IDE

Realizado por: Andrés Solís, Ítalo Parreño, 2019

1.1.8 Aspectos de Seguridad

1.1.8.1 Riesgos, amenazas y Vulnerabilidades en WSN

Observando las amenazas básicas que afectan a un sistema que pretende garantizar la seguridad de la información, en este apartado se particulariza al contexto de las redes inalámbricas de sensores. La principal característica que va a orientar los ataques a estas redes consiste en la naturaleza del medio de comunicación. Las comunicaciones inalámbricas utilizan el espectro electromagnético, por lo que un atacante con la cobertura adecuada podría interceptar la información sin ser detectado. (Asurvey on wireless multimedia sensor networks, 2006)

Adicionalmente, muchas de las aplicaciones de estas redes se desarrollan en entornos no controlados e incluso hostiles, por lo que la seguridad física de los sensores tampoco puede controlarse. De estos dos factores se derivan la mayor parte de los riesgos, los cuales afectarán a la información y a la infraestructura. Las medidas de seguridad han de disponer de los mecanismos necesarios para preservar todos estos aspectos:

- La confidencialidad, debido a la facilidad de acceder al canal de comunicación.
- La autenticidad de la información, ya que se transmite por el aire a todos los dispositivos dentro del área de influencia del emisor.
- La integridad de la información transmitida, para evitar modificaciones accidentales o malintencionadas.
- La vigencia de la información, para evitar la retransmisión de información obsoleta.

- La disponibilidad del canal y de los nodos, evitando ataques de denegación de servicio.
- El acceso lógico a la red, el cual debe ser exclusivo a los nodos designados.
- La captura de algún nodo, siendo necesario que el acceso físico al mismo no permita acceder a la información que contiene.
- Evitar la suplantación de los nodos por dispositivos malintencionados, los cuales pueden afectar la integridad mediante la inyección de información falsa o a la disponibilidad de la red, impidiendo el paso de mensajes legítimos o provocando un consumo descontrolado de los recursos de los nodos.

1.1.8.2 Atributos de Seguridad en WSN

- **Confidencialidad**

La confidencialidad se encarga de mantener el secreto de los datos intercambiados y de garantizar que la información enviada no sea revelada a usuarios no autorizados (intrusos). Además, los usuarios no autorizados no deben ser conscientes de la existencia de datos protegidos ni de su naturaleza. En la figura 22-1 se ve un pequeño ejemplo de cómo alguien puede irrumpir en la confidencialidad de la comunicación entre dos puntos.

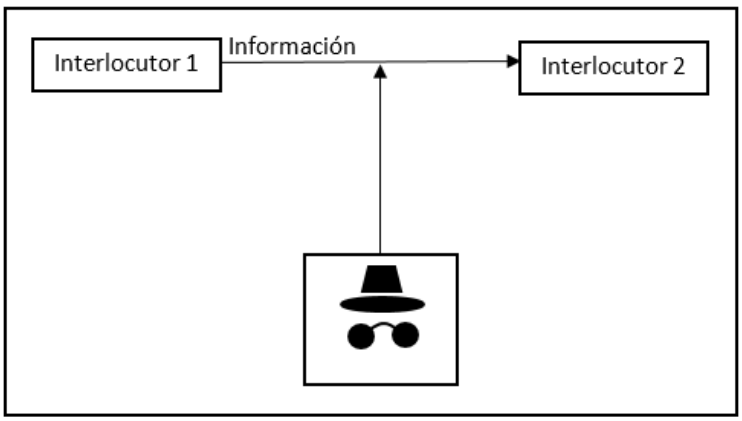

Figura 22-1. Confidencialidad

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Las Redes WSN utilizan el aire como medio de transmisión y esto hace que todos los nodos que se encuentran dentro del rango de transmisión puedan obtener los datos transmitidos, por ello se hace necesario prevenir que nodos intermedios y no confiables tengan acceso o consigan interpretar el contenido de los paquetes que están siendo transmitidos. Cada nodo debe asegurar la información que intercambia con cualquier otro nodo de la Red WSN utilizando mecanismos criptográficos. (Arano, 2010)

- **Autenticación**

La autenticación es una confirmación de que las partes, en comunicación entre sí, son genuinas y no imitaciones, para ello es necesario que los nodos de alguna manera demuestren su identidad. Sin autenticación, un adversario podría enmascarar un nodo y tener acceso a información sensible y clasificada o bien podría interferir con el funcionamiento normal de la red. (Arano, 2010)

En redes de infraestructura o redes inalámbricas con componentes de infraestructura se puede implementar una CA que autentique a los usuarios en un componente de infraestructura. En el caso de las MANETs autónomas o independientes al no existir infraestructura es mucho más difícil autenticar una entidad y se hace necesario utilizar arquitecturas descentralizadas, como ser: CA distribuida total o parcialmente, autenticación basada en ID, Web of Trust, entre otras. Más adelante se describen estas arquitecturas en detalle. (Stallings, 2005)

Existen cuatro tipos de procedimientos de autenticación:

- ❖ Autenticación de la entidad: Garantizar que las entidades (servidores, clientes, personas, etc.) que desean comunicarse con otras sean las que dicen ser.
- ❖ Autenticación de la geo-localización (*Geo-authentication*): La geo-localización de los nodos o cualquier información relacionada con la ubicación debe ser verificada y autenticada.
- ❖ Autenticación de los atributos: Se deben utilizar mecanismos para establecer confianza en los atributos de una entidad o dispositivo.
- ❖ Autenticación de los datos: Es la capacidad que tienen los nodos de comprobar la autenticidad de los datos recibidos.

- **Integridad**

La integridad garantiza que los datos transmitidos entre nodos de la Red WSN sean recibidos por las entidades involucradas sin sufrir modificaciones por parte de terceros y lo que se ha recibido sea lo que originalmente se ha enviado. (Ver Figura 23-1)

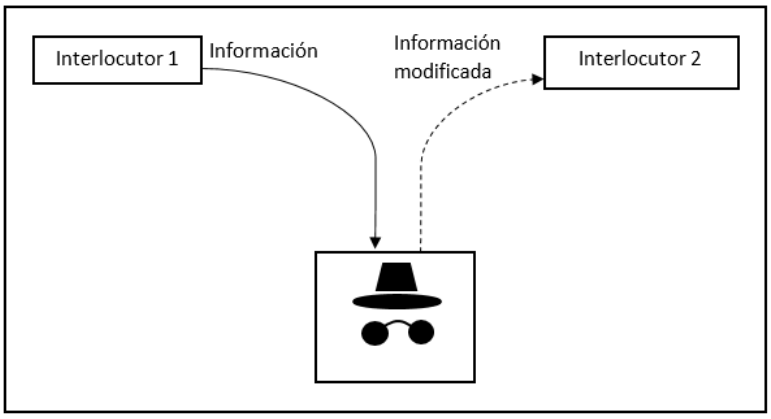

Figura 23-1. Integridad

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En las Redes WSN los datos son enviados a través de medios inalámbricos, por lo tanto, un mensaje se podría corromper debido a razones no maliciosas tales como ruido, interferencias o atenuación de la señal, pero siempre existe la posibilidad que un atacante haya modificado maliciosamente el contenido del mensaje. (Arano, 2010)

1.1.8.3 Algoritmos de Encriptación

- **Cifrado AES**

Advanced Encryption Standard (AES) es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret". Su historia de éxito se inició en 1997, cuando el Instituto Nacional de Estándares y Tecnología (NIST) comenzó oficialmente a buscar un sucesor al envejecimiento cifrado estándar DES. Un algoritmo llamado "Rijndael", desarrollado por los criptografistas belgas Daemen y Rijmen, sobresalía tanto en seguridad como en rendimiento y flexibilidad. (Juan A. Vargas, Lilia García, Sylvia Martinez, Laura Chávez, Diego Muñoz, 2010)

El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada una ejecutada en bloques de datos de 16 bytes - por lo tanto, el término blockcipher. Esas operaciones se repiten varias veces, llamadas "rondas". Durante cada ronda, una clave circular única se calcula a partir de la clave de cifrado y se incorpora en los cálculos.

Basado en la estructura de bloques de AES, el cambio de un solo bit, ya sea en la clave, o en el bloque de texto sin cifrado, da como resultado un bloque de texto cifrado completamente diferente - una ventaja clara sobre los cifrados de flujo tradicionales. La diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES.

- **Cifrado RSA**

Originalmente descubierto en 1973 por la agencia de inteligencia británica GCHQ, recibió la clasificación "top secret". Debemos agradecer a los criptólogos Rivest, Shamir y Adleman por su redescubrimiento civil en 1977. Ellos tropezaron con él durante un intento de resolver otro problema criptográfico. (Stallings, 2005)

A diferencia de los sistemas tradicionales de cifrado simétrico, RSA trabaja con dos claves diferentes: una pública y una privada. Ambos trabajan complementarios entre sí, lo que significa que un mensaje cifrado con uno de ellos sólo puede ser descifrado por su contraparte. Dado que la clave privada no puede calcularse a partir de la clave pública, ésta está generalmente disponible para el público. (Stallings, 2005)

La seguridad de RSA se basa principalmente en el problema matemático de la factorización entera. Un mensaje que está a punto de ser cifrado se trata como un gran número. Al cifrar el mensaje, se eleva a la fuerza de la llave, y se divide con el resto por un producto fijo de dos primos. Repitiendo el proceso con la otra clave, el texto sin formato se puede recuperar de nuevo. (Stallings, 2005)

El mejor método actualmente conocido para romper el cifrado requiere factorizar el producto utilizado en la división. Actualmente, no es posible calcular estos factores para números mayores de 768 bits. Es por eso que los criptosistemas modernos usan una longitud de clave mínima de 3072 bits. (Stallings, 2005)

1.1.9 Estudios de Ondas Sísmicas

1.1.9.1 Ondas Sísmicas

Las ondas materiales (todas menos las electromagnéticas) requieren un medio elástico para propagarse, este medio se deforma y se recupera vibrando al paso de la onda. El punto en donde la perturbación comunica una agitación a la primera partícula del medio en que impacta, es el foco de las ondas y en esa partícula se inicia la onda (Jáuregui, 2005)

Los aspectos más importantes de las ondas son su velocidad de propagación y las codificaciones que sufren cuando:

- Cambian las propiedades físicas del medio en el cual se propagan (difracción, dispersión)
- Se les interpone diferentes clases de obstáculos (difracción, dispersión)
- Varias ondas coinciden en la misma región del espacio (interferencia)

En función del tipo de medio que requieren para su propagación, las ondas se clasifican en: mecánicas y electromagnéticas. Las mecánicas requieren un medio elástico para propagarse y las electromagnéticas no se pueden propagar en el vacío. (Jáuregui, 2005)

Si las clasificamos en función de cómo vibran respecto a la dirección de propagación tenemos las ondas longitudinales y las transversales (Jáuregui, 2005)

✓ Ondas sísmicas

Los sismos son causados por las perturbaciones transitorias del equilibrio de una parte de la tierra que puede producirse por:

- Liberación repentina de energía de deformación al sobrepasar el límite de resistencia del material y producir desplazamientos relativos repentinos en puntos (áreas) localizadas en el interior de la tierra.
- La liberación de energía producido por procesos volcánicos y movimientos de magma o sus productos
- Transmisión de energía al globo terrestre por impactos sobre la superficie terrestre o cambios físicos violentos

En un sólido pueden transmitirse dos tipos de ondas:

- Ondas P (Ver Figura 24-1) llamada también de comprensión, longitudinal o primarias, que consiste en la transmisión de comprensiones y dilataciones, esta onda es de deformación que al paso de un cuerpo solo origina cambio de volumen mas no en su forma. Esta son las primeras en legar por ser más veloces. Estas ondas son capaces de propagarse por medios sólidos y fluidos. (Jáuregui, 2005)
- Ondas S (Ver Figura 25-1) llamadas transversales o de cizallamiento, aquí las partículas se mueven en dirección perpendicular a la dirección de propagación de la onda, esta onda al paso de un cuerpo origina cambio de forma y el volumen permanece constante. Estas ondas pasan a raves del globo terrestre por caminos muy parecidos a los de las ondas longitudinales. la onda transversal no penetra el núcleo, esto permite suponer que parte del núcleo es líquido ya que las ondas S no se propagan a través de medios fluidos.

En sismología, los varios grupos de ondas que representan diferentes tipos de ondas, o grupos de ondas del mismo tipo que llegan a la estación por diferentes caminos, se les llama “fases”. La identificación de las fases (tipo de onda, trayectoria seguida a través de la Tierra) y el tiempo de llegada a la estación sísmica son fundamentales en la interpretación de un sismograma. (Jáuregui, 2005)

Las ondas comprensionales y transversales son llamadas P y S respectivamente. Son conocidas también como ondas internas ya que se propagan en el interior de un sólido elástico.

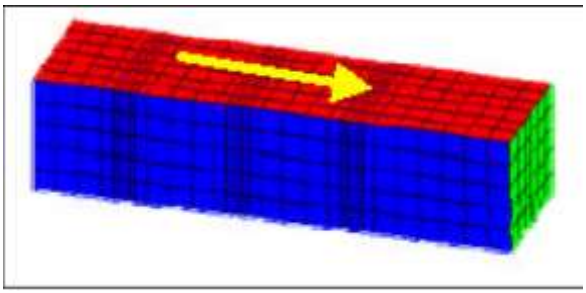

Figura 24-1. Representación gráfica del modo de propagación de la Onda P

Fuente: J. L. M. Jáuregui, 2005, pag. 11

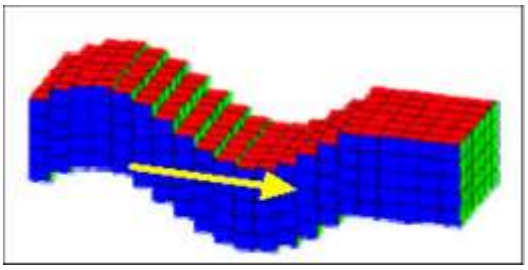

Figura 25-1. Representación gráfica del modo de propagación de la Onda S

Fuente: J. L. M. Jáuregui, 2005, pag. 11

Las velocidades de las diferentes ondas dependen de las características del medio; por ejemplo, en las rocas ígneas la velocidad de las ondas P es del orden de 6 km/s, mientras que en rocas poco consolidadas es de aproximadamente 2 km/s o menor.

Debido a la diferencia en la velocidad de cada tipo de onda, cuando se siente un sismo las primeras sacudidas son debidas a las ondas P, siendo las siguientes ondas S y por ultimo las ondas superficiales. La velocidad de cada tipo de onda es la propiedad que se utiliza para determinar la localización del foco del sismo.

1.1.9.2 Ondas Sísmicas con WSN

En un estudio denominado "**Una red de sensores inalámbricos para el monitoreo de señales volcánico-sísmicas."** Se destacan varias características que en nuestro proyecto nos servirán como un antecedente. (A wireless sensor network for monitoring volcano-seismic signals, 2014)

Las señales sísmicas son recolectadas en la ubicación volcánica de remoción por un conjunto de sensores. Un único nodo especial en el conjunto de sensores, el nodo central, que será detallado más adelante, es el responsable de recolectar todos los datos y transmitirlos a una ubicación remota, por ejemplo, usando una puerta de enlace satelital. Desde este punto se envían las muestras recolectadas al laboratorio volcánico remoto. Allí, personal especializado puede analizar los datos y producir predicciones científicas basadas en el estado actual del evento volcánico.

Geográficamente, la topología propuesta para los experimentos estándar que utilizan la matriz WSN desarrollada se presenta en la Figura 26-1. En esta topología, cada nodo puede realizar una de las tres funciones siguientes. (A wireless sensor network for monitoring volcano-seismic signals, 2014)

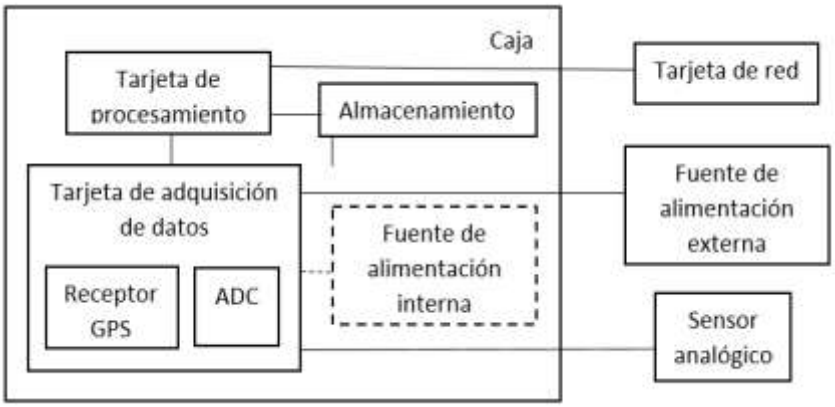

Figura 26-1. Arquitectura de hardware del nodo

Fuente: R. Lopes Pereira, J. Trindade, F. Gonc¸alves, L. Suresh, D. Barbosa, and T. Vazão, 2004, pag. 4.

El nodo central está situado en el centro de la topología para reducir el número máximo de saltos que debe tomar un mensaje de cualquier fuente para llegar a él. Sólo puede existir un nodo central en un momento dado. Un nodo que desempeña esta función tiene un impacto crítico en la red, ya que todos los demás nodos le transmiten los datos recogidos. Por lo tanto, es fundamental que este nodo esté menos expuesto a los daños causados por los diversos peligros naturales presentes en una región volcánica. (A wireless sensor network for monitoring volcano-seismic signals, 2014)

Los nodos que realizan la función intermedia son nodos normales de sensores, pero su ubicación específica se elige de forma que puedan sustituir a los nodos adyacentes en caso de que fallen. Su objetivo es proporcionar un enlace de respaldo para garantizar la comunicación continua con el nodo central. Para que un nodo abarque al menos otros dos nodos.

Finalmente, los nodos pueden tener el papel de nodos sensores. Estos sólo adquieren datos de sus dispositivos sensores y transmiten la información recogida al nodo central o a otro nodo que se encuentre en el camino al nodo del fregadero.

Los nodos del sensor realizarán datos hacia el fregadero para otros nodos que no puedan llegar directamente al nodo central. (A wireless sensor network for monitoring volcano-seismic signals, 2014)

La topología de base propuesta puede ampliarse con nodos sensores adicionales en las extremidades para aumentar el alcance. Es importante notar que a medida que el número de saltos de un sensor al fregadero aumenta, también lo hace el retardo en los paquetes de datos que llegan al nodo central.

1.1.10 Eficiencia Energética

Esta es la relación entre la energía liberada y la energía almacenada, Z ¼ Wut/Wst. Esta definición a menudo se simplifica demasiado porque se basa en un único punto de operación. Sin embargo, los sistemas tienen pérdidas de carga, sin carga y de auto descarga. La definición de eficiencia, por lo tanto, debe basarse en uno o más ciclos realistas para una aplicación específica. (Energy storage systems-Characteristics and comparisons, 2007)

El poder instantáneo es un factor definitorio de la eficiencia. Para que el sistema de almacenamiento sea realmente competitivo, es necesario tener una buena eficiencia general. Esto significa que, para un funcionamiento óptimo, la transferencia de potencia debe tener pérdidas limitadas en términos de transferencia de energía y auto descarga. Las medidas de conservación de energía son un elemento esencial para la nivelación diaria de la carga de la red.

La Figura 27-1 ilustra de forma simplista la existencia de un tiempo de descarga óptimo y una eficiencia máxima. Para los sistemas de almacenamiento reales, estos resultados son más complejos, ya que los elementos de la ilustración varían según el punto de funcionamiento y, en particular, según el estado de carga. (Energy storage systems-Characteristics and comparisons, 2007)

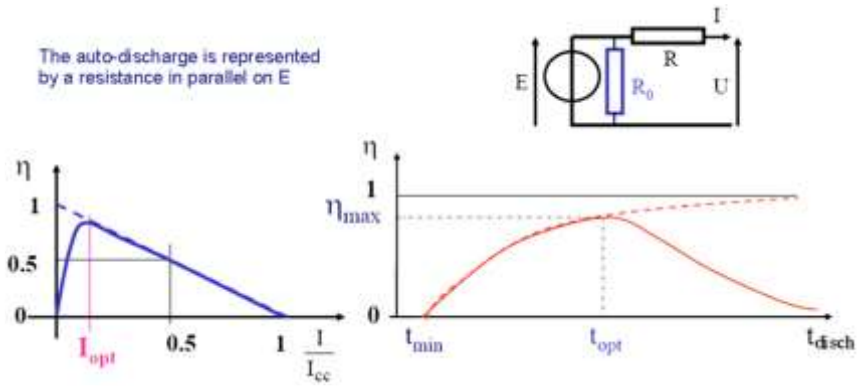

Figura 27-1. Efecto de la corriente o del tiempo de descarga, así como el efecto de la auto descarga en eficiencia del acumulador electroquímico

Fuente: H. Ibrahim, A. Ilinca, and J. Perron, 2009, pag 19

La Figura 28-1 representa el efecto de la corriente o del tiempo de descarga, así como el efecto del auto descarga en eficiencia del acumulador electroquímico. Las líneas punteadas corresponden a un modelo sin auto descarga resistencia (I: fuente de corriente, ICC: corriente de cortocircuito)

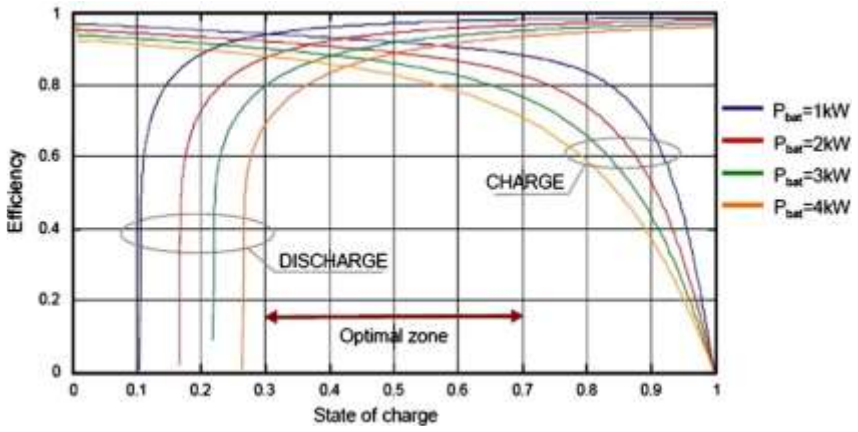

Figura 28-1. Eficiencia energética de una batería de plomo de 48 V-310Ah (15 kWh/10 h de descarga)

Fuente: H. Ibrahim, A. Ilinca, and J. Perron, 2009, pag. 19

Todos los sistemas de almacenamiento están sujetos a fatiga o desgaste por el uso. Este suele ser la principal causa del envejecimiento, antes de la degradación térmica. El diseño de un sistema de almacenamiento que considera la resistencia de la unidad en términos de ciclos debe ser una importancia primordial a la hora de elegir un sistema. Sin embargo, los procesos de fatiga real son a menudo complejos y la capacidad de pedaleo no lo es. Siempre bien definido. En todos los casos, está fuertemente ligado a la amplitud de los ciclos y/o el estado medio de carga. Además, los ciclos generalmente varían mucho, lo que significa que la cuantificación de N es delicada y los valores dados representan órdenes de magnitud

1.1.10.1 Eficiencia Energética en una Red WSN

La eficiencia energética tiene como objetivo maximizar el tiempo de vida de la red WSN, a la vez que la aplicación cumple con sus requisitos de Calidad de Servicio (QoS). En cuanto a mejoras tecnológicas que nos permiten aumentar la capacidad de las baterías presentan un paulatino progreso. Esto provoca que la eficiencia energética siga siendo un reto para este tipo de redes en un futuro. (Moreno, 2013)

Diseñar los nodos para un bajo consumo supone elegir componentes de baja potencia. El primer parámetro a considerar es los consumos de energía de la CPU, el sensor, el radio transceptor y, posiblemente, de otros elementos, como la memoria externa y los periféricos durante el modo normal de operación. (Moreno, 2013)

La selección de piezas de baja potencia, involucra aceptar compromisos sobre el medio. Es regla general que una CPU de potencia baja opera en un ciclo reducido de reloj, con menos características en el chip que otras unidades similares que consumen más energía.

El objetivo básico es la optimización del consumo de energía en los nodos para conseguir el máximo tiempo de vida de la red. Los elementos a valorar: el primer consumidor de energía en la red es la comunicación. Un sistema distribuido indica que varios sensores necesitarán comunicarse a través de largas distancias, lo que significa un mayor consumo en la red. Por ello un método a utilizar es procesar localmente la mayor cantidad de energía, para minimizar el número de bits transmitidos. (Moreno, 2013)

El CPU tiene la capacidad de quedar en estado "sleep" mientras "no se encuentre realizando ninguna acción". Él envió de datos desde los nodos puede ser de tres formas: de modo continuo en intervalos establecidos, dirigido por eventos (envía cuando se cumple una condición) o dirigido por consulta (sólo cuando se solicita). Existen también sistemas híbridos que utilizan una combinación de las formas mencionadas:

- Economizar la distancia de las comunicaciones.
- Técnicas de software: programación eficiente de líneas de código.
- Protocolos de enrutamiento

CAPÍTULO II

2 MARCO METODOLÓGICO

En este capítulo se describe el diseño metodológico que se utiliza para el desarrollo de la propuesta tecnológica, así también se especifican los requerimientos necesarios tanto hardware como software, en donde se definen los elementos, las características y la arquitectura de red más adecuada para realizar el diseño de red WSN que se utiliza para las diferentes pruebas y así dar solución al problema descrito en el presente trabajo de titulación.

2.1 Diseño Metodológico

En el trabajo de titulación la metodología utiliza está basada en una investigación tecnológica experimental de carácter mixto, en donde se aplica el método inductivo para recopilar la información necesaria para determinar las características más adecuadas para que la red WSN que monitoriza Ondas Sísmicas realice su función de forma correcta y eficiente. El método de campo es más óptimo para la recopilación de datos, en donde, durante un periodo de tiempo se obtienen, recogen y analizan los datos obtenidos por los Nodos Sensores de la red.

La propuesta tecnológica tiene carácter mixto, esto se debe a que en el proceso de investigación y en la obtención de datos, se analizan variables tanto cualitativas como cuantitativas. Para obtener el tiempo en que se van a realizar las mediciones en cuanto a la eficiencia energética, nos basamos en el peor movimiento sísmico registrada en la historia, el cual se produjo en Valdivia, Chile el 22 de mayo de 1960, registrando su movimiento de 9,6 en la escala de Richter por un periodo de tiempo de 4 minutos.

A continuación, en este capítulo se muestra la descripción de la red inalámbrica de sensores (Ver Figura 1-2) que monitoriza ondas sísmicas la cual se encuentra encriptada, esta red está conformada por transmisores distribuidos y un receptor.

Cada transmisor cuenta con una tarjeta llamada Waspmote que se encarga de procesar los datos que obtenga, a cual se encuentran conectadas una lámina piezoeléctrica que produce una señal analógica cuando esta se deforma o se desplaza de su eje neutral que nos permite detecta si existe un movimiento de vibración, una batería que brinda alimentación a la tarjeta para que funcione independientemente ya que donde se encuentra colocado el transmisor no existe alimentación fija, además se encuentra conectado un módulo inalámbrico con su respectiva antena que se encarga de enviar una alerta cuando se detecte una vibración prolongada al receptor para que el usuario pueda visualizar los datos obtenidos.

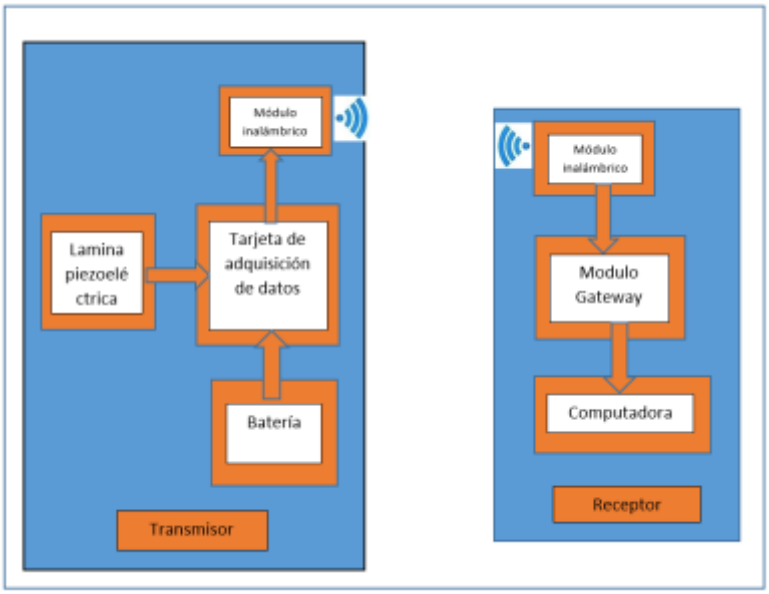

Figura 1-2. Diagrama de Bloques del Sistema

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Para la realización de esta red se consideraron tres aspectos, el nodo sensor conformado por cinco nodos distribuidos en una topología de red en estrella que se encargaran de detectar si existen vibraciones y encriptarlas, el nodo *Gateway* que se encargara de receptar toda la información que envié cada nodo sensor y la computadora donde se des encriptarán los datos para que se puedan visualizar.

2.2 Implementación y Comparación de Consumo entre Topología en Estrella y Topología en Malla

En las tablas 1-2, 2-2, 3-2, 4-2 y 5-2 se muestran los resultados obtenidos durante una hora del consumo energético de una red WSN en topología en Estrella, comparados con una red WSN realizada en la topología en Malla.

Se puede observar como el consumo en la topología en Malla es mucho mayor que la topología en Estrella, debido a que nuestro estudio es la Evaluación de la Eficiencia Energética en comunicaciones encriptadas en una red de sensores inalámbricos WSN que monitoriza ondas sísmicas, necesitamos contar con una topología que no consuma demasiados recursos energéticos, para de esta forma lograr tener un mejor rendimiento en la vida útil de la batería.

Es así que para este trabajo de titulación la topología con la que se diseña la red será la topología en Estrella para poder cumplir con los objetivos planteados.

En la Tabla 1-2 y Tabla 2-2; se detallan los valores de la comparación entre la topología malla y estrella en valores de mA.

.

Tabla 1-2. Comparación entre topología malla vs. estrella en texto plano

Texto Plano	
Distancia 100 metros	
Topología en Malla	Topología en Estrella
Multímetro RadioShack (mA)	Multímetro RadioShack (mA)
80,9	79,6
80,6	74,8
81,3	79,1
81,1	77,7
80,6	79,4
79,5	78,5
81,2	78,5
81	77,6
80,3	78,6
80,6	77,6
81,3	79,7
81,4	76,4
80,6	75,7
79,4	76,2
79,6	79,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 2-2. Comparación entre topología malla vs. estrella en AES 128

AES 128	
Distancia 100 metros	
Topología en Malla	Topología en Estrella
Multímetro RadioShack (mA)	Multímetro RadioShack (mA)
81,9	79,3
80,8	78,2
81,1	80,1
81,2	76
80,3	79,7
80,2	75,7
80,4	76,9
80,7	79,8
80,3	75,9
82	76,9
81	76,5
81,8	79,9
80,6	78,2
81,	75,6
80	77,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 3-2 y Tabla 4-2; se detallan los valores de la comparación entre la topología malla y estrella en valores de mA.

Tabla 3-2. Comparación entre topología malla vs. estrella en AES 192

AES 192	
Distancia 100 metros	
Topología en Malla	**Topología en Estrella**
Multímetro RadioShack (mA)	**Multímetro RadioShack (mA)**
80,2	79,6
84,5	79,2
82,1	80,2
81,8	81,5
84,7	80,3
80,9	80
80,6	78,7
82,3	80,7
81,4	80,6
83,1	78,5
82,7	77,9
80,8	78,5
80,5	79,8
82,4	78,3
81,2	78,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 4-2. Comparación entre topología malla vs. estrella en AES 256

AES 256	
Distancia 100 metros	
Topología en Malla	**Topología en Estrella**
Multímetro RadioShack (mA)	**Multímetro RadioShack (mA)**
82,9	78,3
80	82,3
82,3	80,5
81,7	80,6
81,1	79,5
85,2	82
81	81
83,1	79,8
80,2	80,3
80,4	77,7
81,1	80,8
82	78,5
80,3	81,1
83	81,6
80,9	78,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 5-2; se detallan los valores de la comparación entre la topología malla y estrella en valores de mA.

Tabla 5-2. Comparación entre topología malla vs. estrella en RSA

RSA	
Distancia 100 metros	
Topología en Malla	**Topología en Estrella**
Multímetro RadioShack (mA)	**Multímetro RadioShack (mA)**
82,5	83
82,9	82,8
90,5	82,9
86,6	80,5
83,3	81
82,1	80,9
85,5	82,3
83,2	82,5
84	81,6
82,9	80,8
86,7	81,7
83,8	80,9
83,5	81
82,8	82,6
86,3	81,7

Realizado por: Andrés Solís, Ítalo Parreño, 2019

2.3 Selección de Elementos para la Red

2.3.1 Selección de la tarjeta de adquisición de datos

En la Tabla 6-1 presente en el Capítulo 1 se detalla un Análisis Comparativo de Plataformas para Redes WSN, la cual nos servirá para el proceso de selección. Para evaluar las tecnologías inalámbricas de forma individual se utiliza la escala de Likert, en este método se estima una ponderación comprendida entre 1-5 para establecer el nivel de eficiencia de acuerdo a las características que presentan cada tecnología y que cumplan con los requerimientos de nuestro sistema, la escala de valoración se muestra en la Tabla 1-2:

Tabla 6-2. Escala de Valoración

1	2	3	4	5
Nada Recomendable	No Recomendable	Poco Recomendable	Recomendable	Muy Recomendable
0%	1 – 25%	26 – 50%	51 – 75%	76 – 100%

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Para obtener la eficiencia final de cada plataforma, luego de la ponderación es la fórmula 1 descrita a continuación:

$$P = \frac{Ni}{Ti} * 100\% \quad (1)$$

Dónde:

Ni= Nivel de Incidencia de la característica evaluada

Ti= Total de Incidencias de las Plataformas al nivel 100% de recomendación

Los parámetros de cada una de las plataformas fueron ponderados de acuerdo a las necesidades que nuestro proyecto presenta. En la Tabla 7-2 se puede observar las ponderaciones que designada a cada característica. De los valores obtenidos Waspmote es la tarjeta a utilizarse en el presente trabajo de titulación.

Tabla 7-2. Ponderación de Plataformas para Redes WSN

Dispositivo	Dimensión	µc/CPU	Peso	I/O	SRAM	FLASH	Alimentación
Arduino	1	4	3	2	1	2	1
Raspberry	3	3	2	3	5	4	4
Waspmote	5	4	5	5	1	1	4
	Arduino	Raspberry	Waspmote				
TOTAL	14	24	25				
PONDERACIÓN	40 %	68.57 %	71.45 %				

Realizado por: Andrés Solís, Ítalo Parreño, 2019

De acuerdo a los resultados de la Tabla 7-2, la tarjeta de adquisición de datos que se selecciono fue Waspmote debido a las prestaciones que brinda las cuales son: compatibilidad con los algoritmos de encriptación que se utilizaron, tamaño reducido, dedicado para las redes de sensores inalámbricos como también para ser desplegado en un escenario real, utilizan el mismo entorno de desarrollo y el código que podamos desarrollar para un Arduino lo podremos usar en este dispositivo modificando pequeñas cosas, se adapta a toda clase de sensores por medio de una placa de sensores o conectando directamente a los pines, posee una ranura para la expansión de almacenamiento, cuenta con varias funciones como un *Watchdog*, RTC, acelerómetro integrado, así como también los diferentes modo de funcionamiento de bajo consumo de energía. Trabaja con distintas tecnologías de comunicación inalámbrica tales como WIFI, Bluetooth, Zigbee entre otras.

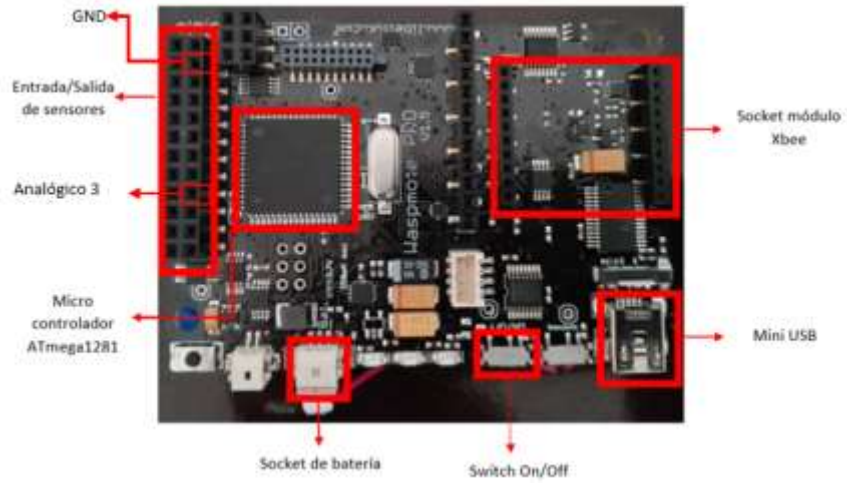

Figura 2-2. Estructura Hardware Waspmote

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Como se muestra en la figura 2-2, para la conexión de la lámina piezoeléctrica utilizamos los pines GND y el analógico 3 para la recolección de los datos, como estamos leyendo de forma analógico esta se codifica como un numero entero 0 y 1023, de esta manera y para evitar falsas alarmas utilizamos tres tipos de vibración las cuales son: movimiento leve (cuando el valor medido va desde 300 a 500), movimiento medio (cuando la medida va desde 600 a 800) y movimiento fuerte (cuando la medida es igual o mayor que 900), esta última alerta creara una trama que está acompañada de la etiqueta del sector donde ocurrió el movimiento sísmico, posteriormente será encriptada y enviada por medio del módulo Xbee.

2.3.2 Selección de la tecnología inalámbrica

En la Tabla 9-1 del Capítulo 1 se encuentra el Análisis comparativo entre las Tecnologías Inalámbricas las cuales serán utilizadas para el proceso de selección. Para evaluar las tecnologías inalámbricas de forma individual se utiliza la escala de Likert, en este método se estima una ponderación comprendida entre 1-5 para establecer el nivel de eficiencia de acuerdo a las características que presentan cada tecnología y que cumplan con los requerimientos de nuestro sistema, la escala de valoración se muestra en la Tabla 8-2:

Tabla 8-2. Escala de Valoración

1	2	3	4	5
Nada Recomendable	No Recomendable	Poco Recomendable	Recomendable	Muy Recomendable
0%	1 – 25%	26 – 50%	51 – 75%	76 – 100%

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Para obtener la eficiencia final de cada plataforma, luego de la ponderación es la fórmula 1 descrita a continuación:

$$P = \frac{Ni}{Ti} * 100\% \quad (1)$$

Dónde:

Ni= Nivel de Incidencia de la característica evaluada

Ti= Total de Incidencias de las Plataformas al nivel 100% de recomendación

Los parámetros de cada una de las plataformas fueron ponderados de acuerdo a las necesidades que nuestro proyecto presenta. En la Tabla 9-2 se puede observar las ponderaciones que nosotros designamos a cada característica.

Tabla 9-2. Ponderación de las tecnologías inalámbricas

Comparación entre Tecnologías Inalámbricas			
	WiFi (IEEE 802.11g)	**Bluetooth (IEEE 802.15.1)**	**ZigBee (802.15.4)**
Radio	4	3	4
Velocidad	5	2	1
Número de Nodos por Máster	1	1	5
Latencia	2	1	5
Tipos de Datos	5	4	1
Alcance (m)	5	1	5
Expansión	5	1	5
Duración de la Batería	1	1	5
Total de Incidencias	28	14	31
Ponderación final	70 %	35 %	82.5 %

Fuente: Andrés Solís, Ítalo Parreño, 2019

Para el módulo de comunicación se optó por la tecnología Xbee que pertenece al estar 802.15.4 Zigbee gracias a su bajo costo, la cobertura que ofrece, el bajo consumo de energía que requiere para su funcionamiento, fácil obtención en el mercado y su tasa de transmisión de datos. Este módulo será el encargado de enviar y recibir los datos entre el nodo sensor y en nodo *Gateway* que envíen los sensores de vibración.

- Módulo Xbee Pro S1

Estos módulos (Ver Figura 3-2) poseen una cobertura entre 60 y 90 metros en interiores/ zonas urbanas y de 750 a 1600 metros en exteriores con línea de vista, este parámetro nos será de gran ayuda para una óptima comunicación entre los diferentes nodos sensores y el nodo *gateway*, además cuentan con una tasa de transmisión de 250 kbps. Para ayudar en la maximización de la cobertura viene incorporado un conector RP-SMA a la cual podemos agregar una antena (Ver Figura 4-2) según el requerimiento.

Figura 3-2. Módulo XBee PRO S1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Figura 4-2. Antenas Módulo XBee PRO S1 de 2400 MHz

Realizado por: Andrés Solís, Ítalo Parreño, 2019

2.3.3 Selección del Sensor

- Lamina piezoeléctrica LDT0-028K

  Esta lámina es seleccionada debido a su funcionamiento ya que si la lámina deja vibrar en el espacio libre crea una tensión de flexión, comportándose, así como un acelerómetro o en nuestro caso un sensor de vibración.

Figura 5-2. Sensor LDTO-028K

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la figura 5-2 podemos observar que este sensor es pequeño y gracias a esto podemos colocarlo donde sea requerido sin quitarnos espacio, para un mejor funcionamiento añadimos al extremo de la lámina una masa que permitirá que cuando la superficie vibre, esta capte de mejor manera el movimiento obteniendo mejores resultados.

Es necesario que este sensor se encuentre bien colocado (completamente extendido), de otra manera a pesar de que no exista movimiento alguno enviara mediciones aleatorias si se encuentra desplazado de su eje neutral, ya que tiene una sensibilidad alta.

2.3.4 Selección de los Algoritmos

En cuanto a los algoritmos que utilizaremos en el presente trabajo son Simétrico y Asimétrico, protegiendo la confidencialidad de nuestra información. Es así que los algoritmos seleccionados para la encriptación de los datos son AES en sus diferentes longitudes de la clave que son: 128, 192 y 256 en cuanto a simétrico y RSA en el asimétricos, son los algoritmos que la tarjeta Waspmote nos permite programar de manera nativa, sin la necesidad de agregar más hardware para encriptar datos y enviarlos de manera inalámbrica.

2.4 Desarrollo del Proyecto

2.4.1 Fases para el Desarrollo del Proyecto

En la Figura 6-2 se muestra las fases que se siguieron para ejecutar el proyecto presente y así obtener los datos para procesar y obtener resultados necesarios para culminar el estudio.

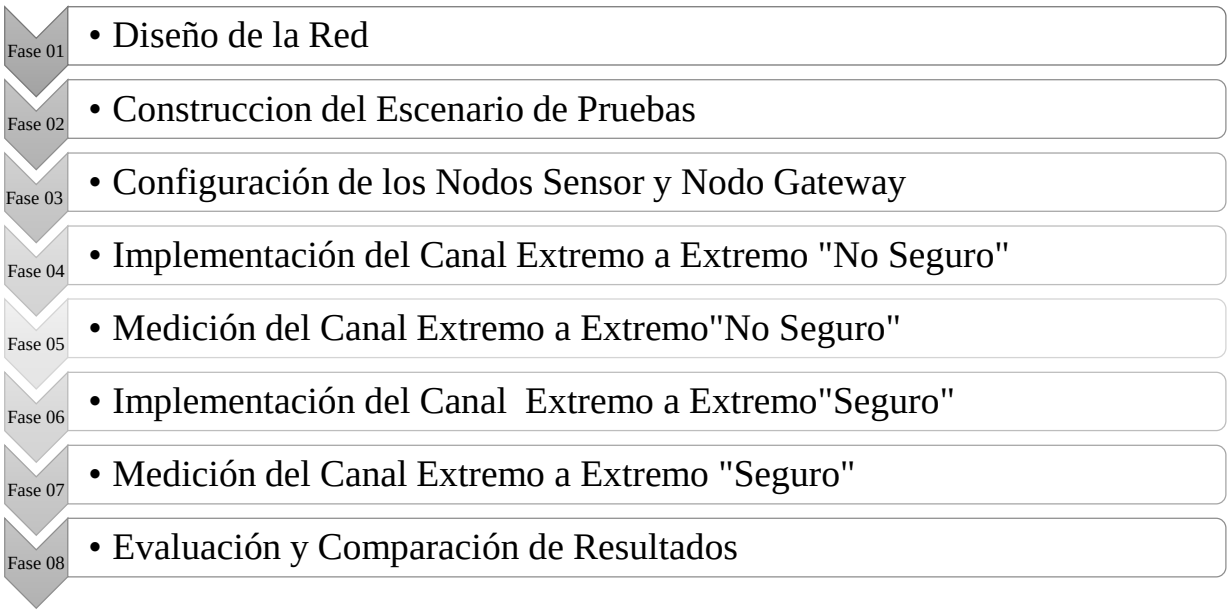

Figura 6-2. Fases de Desarrollo del Proyecto

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- FASE 01: DISEÑO DE LA RED

  En cuanto al diseño de la red, se hizo una previa comparación (Ver Tabla 4-1) entre las características de las diferentes topologías, decidiendo utilizar la topología en Estrella por sus características. Es así que utilizamos Cinco Sensores y un nodo *Gateway* para el establecimiento de la topología en estrella. La comunicación que en la red es unidireccional, esto significa que solo uno de los elementos puedo enviar información y el otro recibir la información. Cada Nodo Sensor envía su información al Nodo *Gateway* como se puede ver en la Figura 7-2.

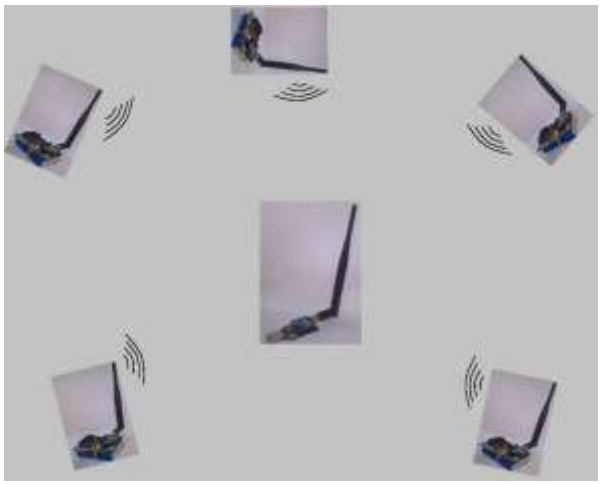

Figura 7-2. Topología de la Red

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Los diagramas de bloques de la Figura 8-2 y la Figura 9-2 nos muestran de manera lógica como están constituidos los Nodos Sensor y Nodo *Gateway*.

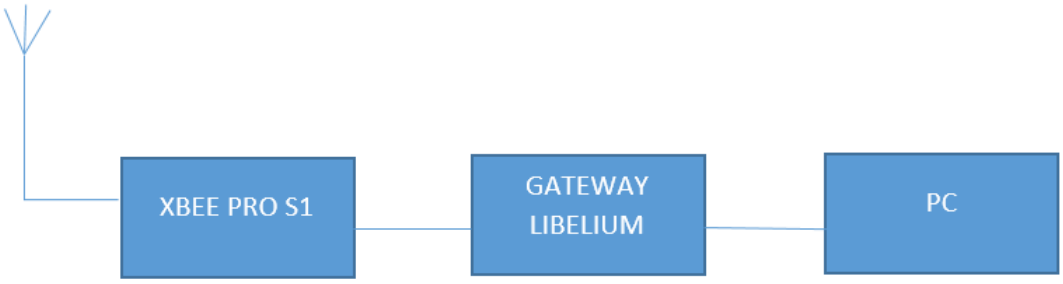

Figura 8-2. Diagrama de bloques Nodo Gateway

Realizado por: Andrés Solís, Ítalo Parreño, 2019

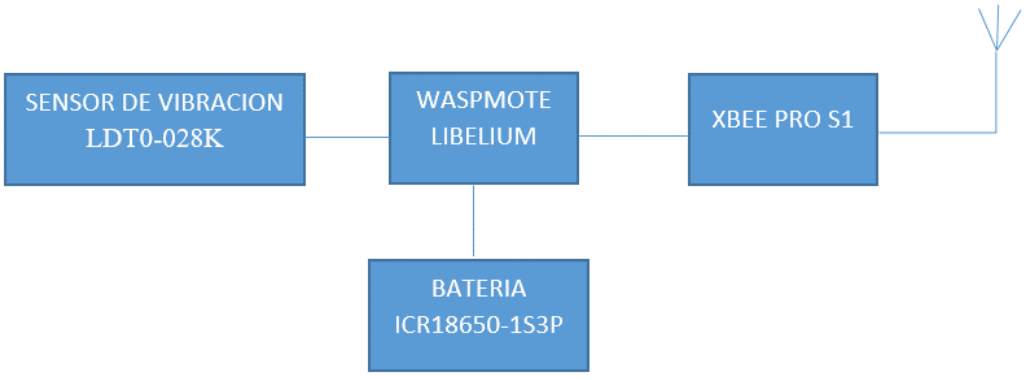

Figura 9-2. Diagrama de bloques Nodo Sensor

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- FASE 02: Construcción del escenario de pruebas

Al tener un escenario que debe simular diferentes movimientos telúricos o movimientos que generan una cierta vibración para que el sensor se deforme y detecte esas vibraciones. Se construyó una maqueta con 5 sectores como se muestra en la Figura 10-2, los cuales representan cada uno un Nodo Sensor.

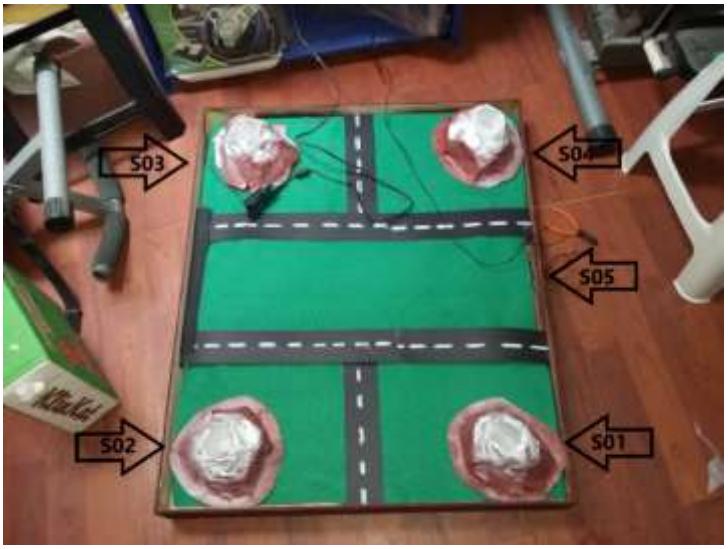

Figura 10-2. Maqueta para realización de pruebas

Realizado por: Andrés Solís, Ítalo Parreño, 2019

El tamaño de la maqueta es 79,5 cm de largo y 66 cm de ancho. Construida con madera, en la Figura 11-2 se observa el marco y base de la maqueta, la cual aporta mayor estabilidad cuando se genere las vibraciones.

Figura 11-2. Marco y Base de la Maqueta

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Cada placa tiene un motor incorporado con una centrina como en la Figura 12-2 se puede observar, la cual es utiliza en elementos que generen vibraciones, como en los controles de videojuegos o en dispositivos móviles; el cual al momento de empezar a funcionar genera vibraciones.

El tamaño de cada placa es 31 cm de largo y 20 cm de ancho. Para sostener cada placa se tiene pernos que ayudan al movimiento libre de cada placa, esto nos permite tener un espacio entre la base y el motor de cada placa.

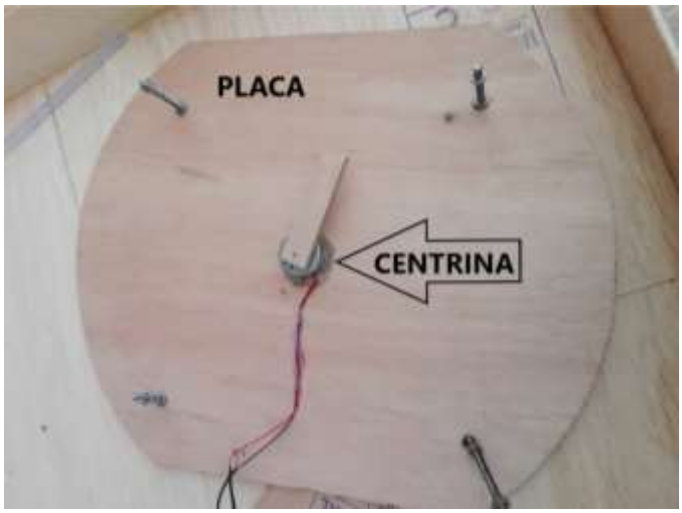

Figura 12-2. Marco y Base de la Maqueta

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Por otro lado, para tener varios niveles de movimientos de las placas, se controla la velocidad del motor con un circuito que nos genere pulsos PWM, en la Figura 13-2 se muestra el esquema del circuito electrónico, así como sus componentes, el dispositivo electrónico encargado de generar los pulsos PWM es el circuito integrado 555.

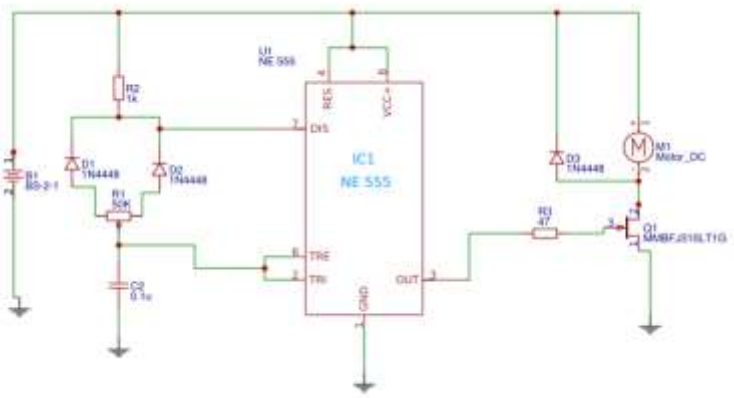

Figura 13-2. Circuito Electrónico del PWM

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- FASE 03: Configuración de los Nodos Sensor y Nodo *Gateway*

✓ Configuración del Nodo Sensor

Para la configuración de los nodos Sensores de igual forma que para el nodo *Gateway* se utiliza el software XCTU para la configuración de los siguientes parámetros en el XBee PRO:

- El canal de comunicación a utilizar es el Canal C.
- El PAN ID el cual es 4040
- Se escribe la dirección MAC del nodo Coordinador que es 0013A20040D7CE50, para que toda la información de los nodos sea direccionada a esa. En XCTU la dirección MAC se escribe de la siguiente forma:
  - **DH** Destination Address High 13A200
  - **DL** Destination Address Low 40D7CE50
- Se designa la función que el dispositivo va a cumplir en la red, siendo el dispositivo final de la red.

Las direcciones MAC de los cinco XBee PRO de los Nodos Sensores utilizados en el estudio se detallan en la Tabla 10-2.

Tabla 10-2. Direcciones MAC de los Nodos Sensores

Número de Sensor	Identificador	Dirección MAC
S01	1010	0013A20040D7CE58
S02	1015	0013A20040D7CE16
S03	1060	0013A20040D7CE20
S04	1050	0013A20040D7CE22
S05	1030	0013A20040D7CE1D

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Para la programación de los diferentes algoritmos el software que utilizamos es WASPMOTE IDE, en la Figura 14-2 se observa las configuraciones iniciales como son las librerías necesarias que se utilizaron para los diferentes programas, la dirección MAC del Nodo *Gateway*, declaración de las variables y la etiqueta que se le da a cada nodo.

Figura 14-2. Interfaz WASMOTE IDE (Nodo Sensor)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Al terminar las configuraciones de los XBee PRO de los nodos tanto el *Gateway* como la de los Sensores en el software XCTU oprimimos en la opción llamada Añadir un Módulo de Radio, esta opción permite que el XBee PRO del Nodo *Gateway* sea leído y una vez añadido en la lista, buscamos la opción de descubrir Módulos de Radio que estén conectados a la dirección MAC del XBee PRO del *Gateway*.

En la Figura 15-2 luego de lo detallado se puede visualizar como los cinco XBee PRO ya configurados son descubiertos y añadidos a la lista de Módulos de Radio de XCTU.

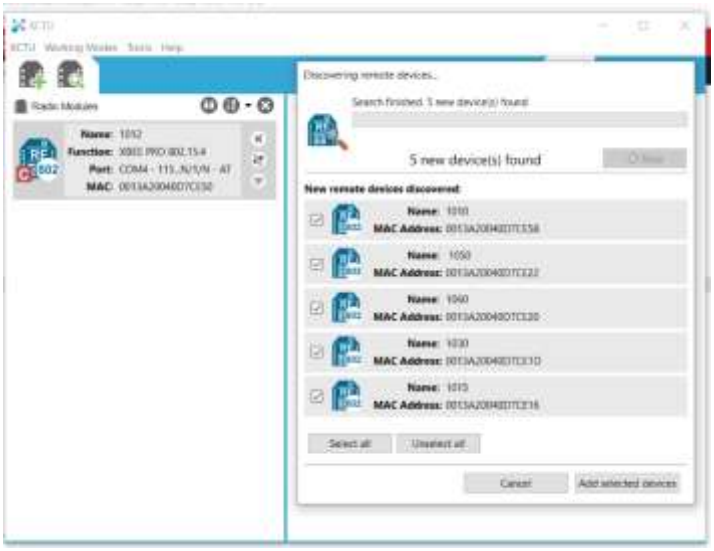

Figura 15-2. Comunicación de los Nodos Sensores y Nodo Gateway

Realizado por: Andrés Solís, Ítalo Parreño, 2019

✓ Configuración del Nodo *Gateway*

En el Nodo *Gateway* para establecer la comunicación inalámbrica se configura el XBee PRO mediante el software XCTU, los parámetros que se deben configurar son: Canal de transmisión, Pan ID, Dirección MAC, Función a cumplir. La dirección MAC del XBee PRO del Nodo *Gateway* es 0013A20040D7CE50, en la Figura 16-2 se puede observar cómo está configurado la dirección MAC, el Canal de Comunicación y el PAN ID.

Figura 16-2. Interfaz gráfica XCTU (Nodo Gateway)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Una vez escrita la dirección MAC configuramos el canal que vamos a utilizar para la comunicación, designando el canal C para la comunicación inalámbrica, lo siguiente a configurar es el PAN ID que es 4040 como se puede observar en la Figura 17-2, al ser el Nodo *Gateway* la función que se configuro fue la de Coordinador, recibiendo así toda la información de los nodos sensores, esto se puede ver en la Figura 18-2.

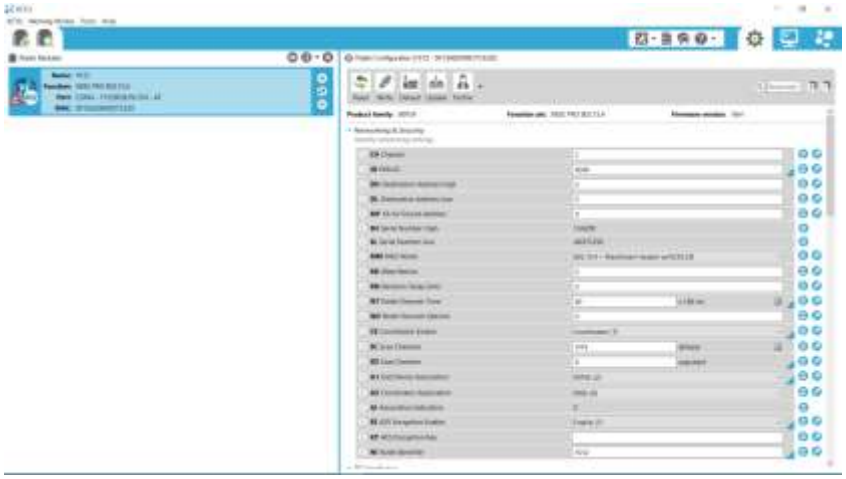

Figura 17-2. Interfaz gráfica XCTU (Nodo Gateway)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

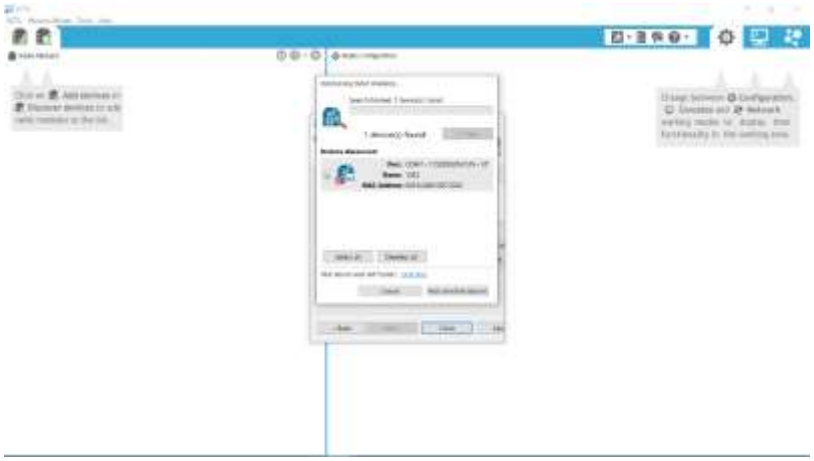

Figura 18-2. Interfaz gráfica XCTU (Nodo Gateway)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- FASE 04: Implementación del Canal Extremo a Extremo "No Seguro" en la Red WSN que monitoriza Ondas Sísmicas

  La Implementación del Canal Extremo a Extremo "No Seguro" en la Red WSN que monitoriza Ondas Sísmicas se puso en funcionamiento los Nodos Sensores, con el primer programa que nos envía nuestro mensaje en texto plano, es decir sin una encriptación del mensaje. (Ver Anexo C)

Figura 19-2. Canal Extremo a Extremo "No Seguro"

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Entonces para que la red se encuentre en un canal No Seguro que en la Figura 19-2 se puede notar, basta con configurar la dirección del Nodo *Gateway* y subir el programa que desarrollamos para detectar las vibraciones que el sensor reciba de acuerdo a los movimientos de cada placa en nuestro escenario de pruebas, las librerías que se utilizan en el programa son:

- #include "WaspXBee802.h"
- #include "WaspFrame.h"

Para poder detectar las vibraciones con el sensor, leemos los cambios que se generan en voltajes al momento de cambios en voltajes, esto se produce ya que al momento de que el sensor sale de su eje neutral, produce un valor que es leído de forma analógico, el mínimo valor del sensor al estar en su posición neutral es 0 y al momento de mayor torsión es 1023.

Mediante esos valores podemos definir un variable llamada val = analogRead(ANALOG3); en donde analogRead(ANALOG3) es la sentencia usada para la lectura de los valores de nuestro sensor, en la variable dicha se recogen los valores, luego definimos condiciones para cada mensaje que queremos que se visualice, esto se detalla en la Tabla 11-2. (Ver Anexo A)

Tabla 11-3. Direcciones MAC de los Nodos Sensores

Nº	Condición	Salida
01	val < 250	Espacio en Blanco
02	(val >= 300) & (val <= 500)	Movimiento Leve
03	(val >= 600) & (val <= 800)	Movimiento Medio
04	val >= 900	Movimiento Fuerte !Alerta!

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Se decidió por estas condiciones debido a que en nuestro escenario de pruebas vamos a simular diferentes casos reales que se han registrado al pasar de los años con respecto a los movimientos telúricos. Es así que la primera condición donde nuestro contador llegue a ser menor de 250, simula un movimiento producido por maquinaria, vehículos pesados y demás movimientos que no lleguen a los 1,5 Grados en la escala de Richter siendo esta medida en condiciones reales. En cuanto a la segunda condición se da cuando el contador sea mayor o igual a 300 y cuando sea menor o igual a 500, se imprimirá el mensaje de Movimiento Leve lo cual representa un movimiento menor de 3,5 Grado en la escala de Richter. El mensaje de Movimiento Medio se visualizará en el monitor serie cuando las perturbaciones detectadas por nuestro sensor sean mayores o iguales a 600 y menor o igual a 800, esto representa a un movimiento real comprendido entre 3,5 a 6 Grados en la escala de Richter. Por último, el mensaje Movimiento Fuerte ¡Alerta¡, siendo este el mensaje que se enviara de manera inalámbrica mediante la XBee PRO, se genera cuando los datos obtenidos del sensor sean contados mayor que 900 en el programa, se simula con nuestro prototipo un movimiento comprendido entre 6,1 Grados a 12 Grados en la escala de Richter.

- FASE 05: Medición del Canal Extremo a Extremo “No Seguro” y del Canal Extremo a Extremo “Seguro” de la Red WSN que monitoriza Ondas Sísmicas.

  La medición del Canal Extremo a Extremo “No Seguro” y del Canal Extremo a Extremo “Seguro” de la Red WSN que monitoriza Ondas Sísmicas, simulara el peor movimiento sísmico registrada en la historia, el cual se produjo en Valdivia, Chile el 22 de mayo de 1960, registrando su movimiento de 9,6 en la escala de Richter por un periodo de tiempo de 4 minutos.

  Los datos que obtendremos de las mediciones en el Nodo Sensor, se las realizaran mediante 2 diferentes dispositivos siendo dos multímetros un RadioShack y otro de marca genérica, se tiene estos dos dispositivos para poder comparar y ver cuanta diferencia produce en las medidas, ya que los dos dispositivos tienen componentes diferentes. Para el Nodo *Gateway* utilizamos el dispositivo Keweisi.

  Al tener una población infinita, para poder obtener la muestra que nuestro experimento necesita realizamos una muestra piloto de 30 datos, para poder de estar manera tener una muestra total, la cual nos permitirá conocer cuántas veces debemos realizar nuestro experimento y obtener los datos necesarios para cumplir con los objetivos del estudio.

De la muestra piloto los datos tienden siempre a tener una distribución normal esto debido al Teorema del Limite Central, el cual nos dice que en condiciones muy generales los datos se aproximan siempre a una distribución normal. Es por ello que el valor de α= 0,05 y el cuantil de esta zona es de 1.96.

En la Tabla 12-2 se encuentran los valores de la varianza de la muestra piloto (Ver Anexo B) de cada dispositivo con el que realizamos las mediciones, estos valores fueron calculados por un software estadístico denominado R.

Tabla 12-2. Varianza de la Muestra Piloto

Algoritmo	Varianza Multímetro Genérico	Varianza Multímetro Radioshack
Texto Plano	3.865299	2.792471
AES 128	2.792471	4.032195
AES 192	0.9835517	2.443506
AES 256	1.761195	2.225161
RSA	1.82823	0.7562759

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 13-2 se encuentran los valores de la desviación estándar de nuestra muestra piloto, los valores se obtienen de la fórmula 2.

$$S = \sqrt{\sigma^2} \quad (2)$$

Tabla 13-2. Desviación Estándar de la Muestra Piloto

Algoritmo	Varianza Multímetro Genérico	Varianza Multímetro Radioshack
Texto Plano	3.865299	2.792471
AES 128	2.792471	4.032195
AES 192	0.9835517	2.443506
AES 256	1.761195	2.225161
RSA	1.82823	0.7562759

Realizado por: Andrés Solís, Ítalo Parreño, 2019

La fórmula 3 obtenemos el error de precisión, donde utilizamos el 15% de S (Desviación Estándar), los datos obtenidos se tienen en la Tabla 14-2.

$$e = |\mu - \bar{x}| = 15\%S \quad (3)$$

Tabla 14-2. Error de Precisión

Algoritmo	Error	Error
Texto Plano	0.57979485	0.41887065
AES 128	0.41887065	0.60482925
AES 192	0.147532755	0.3665259
AES 256	0.26417925	0.33377415
RSA	0.2742345	0.113441385

Realizado por: Andrés Solís, Ítalo Parreño, 2019

De la fórmula 4 como resultado tenemos la muestra mínima para nuestra población infinita, es decir que se deben realizar 171 mediciones como mínimo, nuestro escenario de pruebas compuesto por el prototipo de la red WSN, el cual es un prototipo para un estudio de laboratorio, nos permite simular el peor sismo registrado que ha sido previamente descrito.

$$n = \left(Z_T * \frac{S}{0.15S}\right)^2 = \left(\frac{Z_T}{0.15}\right)^2 \quad (4)$$

$$n = \left(\frac{1.96}{0.15}\right)^2 = 170.73 = 171\ muestras$$

Se simula un movimiento que nuestro sensor detecta como un movimiento fuerte debido a la programación, mas no se simula una onda real, debido a que para simular el movimiento real de una onda se debe realizar un estudio más profundo de ondas, pero nuestro estudio no se centra en la simulación de ondas sísmicas, el fin del estudio es la eficiencia energética.

Al ser el peor sismo registrado de una duración de 4 minutos, tomamos este tiempo para la toma de mediciones, es decir que en una hora se tendrá 15 datos; de esta forma para obtener 50 datos se necesitaran de 200 minutos o 3 horas con 20 minutos de trabajo constante de la tarjeta.

Al tener 5 diferentes formas de envió de nuestro mensaje: Texto Plano, AES 128, AES 192, AES 256 y RSA, el tiempo necesario de trabajo de las tarjetas son de 13 horas con 20 minutos; es por ello que nosotros vamos a tomar 200 mediciones es decir que se van a tomar cuatro días para obtener los 200 datos que necesitamos para poder conocer cual algoritmo nos otorga un equilibrio entre la eficiencia energética y la seguridad.

Para medir el consumo en el *Gateway* la conexión es conectando el dispositivo Keweisi directamente a un puerto USB del computador y en uno de los dos slots del dispositivo conectar y así obtendremos los valores que el *Gateway* consumo al momento de recibir los datos de los nodos. Esto se puede ver de mejor forma en la Figura 20-2.

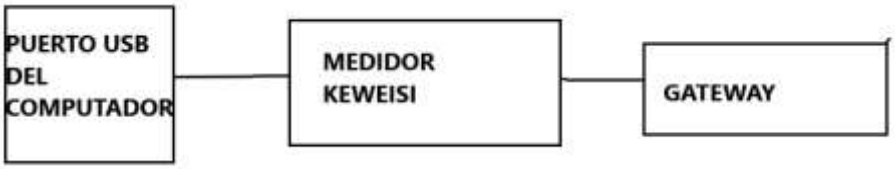

Figura 20-2. Esquema de Conexión del Gateway

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En cuanto a la manera que en el Nodo Sensor se va a tomar las mediciones, el esquema para medir con los otros dispositivos que son los diferentes multímetros se muestra en la Figura 21-2.

Figura 21-2. Esquema de Conexión del Multímetro

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Figura 22-2 se muestra el esquema de distancia para las pruebas. Se tomó la distancia de 100 metros debido a que es la distancia máxima que el XBee Pro soporta.

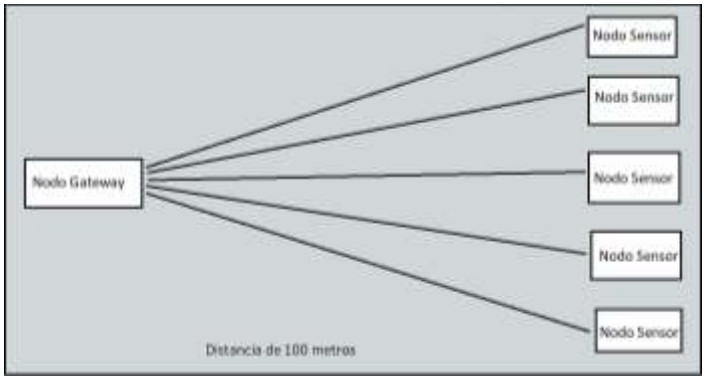

Figura 22-2. Esquema de Conexión del Multímetro

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- FASE 06: Implementación del Canal Extremo a Extremo “Seguro” en la Red WSN que Monitoriza Ondas Sísmicas

  Tener un canal “Seguro” en una comunicación inalámbrica que envía datos que son de carácter sensible nos garantiza que esa información va a llegar a su destino de manera correcta sin ninguna alteración. Para ello se aplica algoritmos de encriptación, de los algoritmos de encriptación se tiene 2 tipos: Asimétrico, Simétrico.

  - El algoritmo Asimétrico que fue seleccionado para el proyecto es AES ya que las tarjetas Waspmote nos permite trabajar con este tipo de encriptación, las tarjetas poseen 3 diferentes tipos de longitud de las llaves, siendo estas de 128,192 y 256.

    Al tener waspmote de forma nativa el proceso de encriptación sea de un paquete o de un vector de caracteres no necesita de ninguna placa o accesorio extra para encriptar la información que nosotros deseamos.

    La librería que waspmote utiliza para el proceso de encriptación en cuanto a AES es la siguiente **#include <WaspAES.h>** la cual necesita de una llave o password para producir la encriptación del paquete.

    El paquete a encriptar será la alerta de que se está detectando un movimiento telúrico de una magnitud elevada. La cual es “SISMO S01” donde S01 indica el sector en donde se está detectando el movimiento, luego de cumplir las condiciones que han sido programadas.

    Este comando es el que nos permite encriptar nuestra información **frame.encryptFrame(AES_192, password)** reemplazando el tamaño de la llave**,** y luego de ser encriptada esa información que tiene un tamaño de 61 bits se envía de manera inalámbrica a través del ZigBee, en la Figura 23-2 se puede ver el mensaje encriptado enviado. (Ver Anexo C)

Figura 23-2. Canal Extremo a Extremo "Seguro" (AES)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

- Para la encriptación utilizando un algoritmo Simétrico se utiliza RSA que con las Tarjetas Waspmote podemos encriptar información, en el que se requieren de dos llaves una privada y una pública. RSA realiza el proceso de encriptación teniendo toda su información en hexadecimal. (Ver Figura 24-2)

Figura 24-2. Canal Extremo a Extremo "Seguro" (RSA)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

La librería que waspmote utiliza para realizar esta encriptación es **#include <WaspRSA.h>.** La llave está definida como un formato Hexadecimal de la siguiente forma 0x00010001 = 65537, de un numero primo.

La longitud de llave que RSA maneja es 1024 el cual es la longitud recomendada para tener una seguridad robusta. Se puede utilizar de un número menor a eso, en nuestro proyecto se utiliza la longitud de llave de 1024, el cual para poder desencriptarlo toma un tiempo considerable. (Ver Anexo C)

Con este comando se **RSA.encrypt(message, public_exponent, modulus, enc_message, sizeof(enc_message));** se realiza la encriptación de la información, el tamaño de la información … que nosotros deseamos enviar de forma inalámbrica.

- FASE 08: Evaluación y Comparación de resultados

Una vez terminadas las pruebas realizadas durante 13 horas con 20 minutos, se obtuvieron dos cientos valores de corriente, en texto plano y con los algoritmos de encriptación previamente detallados; en una distancia de 100 metros. Estos datos fueron tabulados, se obtuvo una media de los cincuenta datos, la media de los datos es presentada en gráficas para una mejor presentación de los resultados.

Los resultados obtenidos en el Nodo Sensor se comparan entre las tres herramientas medidoras, esto nos permitió conocer cuál de los de las herramientas nos entrega valores más exactos en cuanto a la eficiencia energética. La comparación se hizo entre texto plano con cada uno de los algoritmos de encriptación: AES 128, AES 192, AES 256 y RSA.
De esta forma se pudo observar cuál de los algoritmos de encriptación previamente detallados nos proporciona un equilibrio entre eficiencia energética y la seguridad presente en red para asegurar la confidencialidad de los datos enviados de manera inalámbrica.

2.5 Eficiencia Energética

En cuanto a la eficiencia energética el cual es el motivo de estudio, la definimos como la relación entre la energía liberada y la energía almacenada de un dispositivo que alimenta al conjunto que forma el nodo sensor.

Se realizaron tres diferentes mediciones en nuestra red de estudio:

- La primera medición fue realizada mediante una comunicación en texto plano, entre los nodos sensores y el nodo *Gateway* para poder conocer cuánto es el consumo del nodo *Gateway* al momento de procesar todos los datos y del nodo Sensor al momento del envió.
- La segunda medición realizada fue en una comunicación aplicando un algoritmo de encriptación: AES con sus diferentes tipos de llaves 128,192 y 256, midiendo de igual forma el consumo en los nodos sensores y en el nodo *Gateway*.
- La tercera medición se la hizo en una comunicación encriptada aplicando RSA, obteniendo datos de consumo del nodo *Gateway* y del nodo sensor.

Para poder realizar estas medidas nos ayudamos de una herramienta desarrollada por la empresa Keweisi, el cual nos permite obtener valores de corriente en Amperios que el Nodo *Gateway* consume al momento de recibir los datos enviados por cada uno de los sensores. En el nodo Sensor se utilizó dos multímetros de diferentes marcas y características que anteriormente han sido detallados.

CAPÍTULO III

3 MARCO DE RESULTADOS

En este capítulo se describe el proceso necesitado para realizar las mediciones sobre el escenario de pruebas, de igual forma el análisis de los datos obtenidos de las mediciones, permitiendo así conocer la Eficiencia Energética de cada tipo de dato enviado.

3.1 Resumen de las pruebas realizadas

Para obtener los resultados de la transmisión de datos en texto plano y cada algoritmo, se realizaron doscientas mediciones de cada uno con dos diferentes medidores: un multímetro genérico Serie 830 y un multímetro RadioShack, en cada uno de los nodos sensores y un medidor Keweisi para el nodo *Gateway* con una duración de cuatro minutos para cada medición, en la Tabla 1-3 se encuentra el resumen del experimento realizado.

Tabla 1-3. Resumen De Los Experimentos Realizados (Horario para los cuatro días)

Periodo de Tiempo	Día	Distancia	Algoritmo
8:00 a 23:20	Viernes	100 m	RSA
8:00 a 23:20	Sábado	100 m	AES 256
8:00 a 23:20	Domingo	100 m	AES 192
8:00 a 23:20	Lunes	100 m	AES 128
8:00 a 23:20	Martes	100 m	Texto Plano

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2 Mediciones en el Nodo *Gateway*

En la Figura 1-3 y la Figura2-3 se ve como se toman las medidas en el Nodo *Gateway* con ayuda del dispositivo medidor Keweisi.

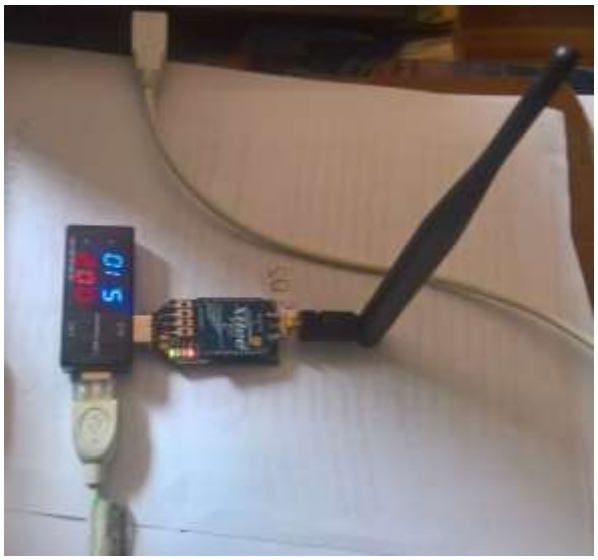

Figura 1-3. Medición en el Nodo Gateway

Realizado por: Andrés Solís, Ítalo Parreño, 2019

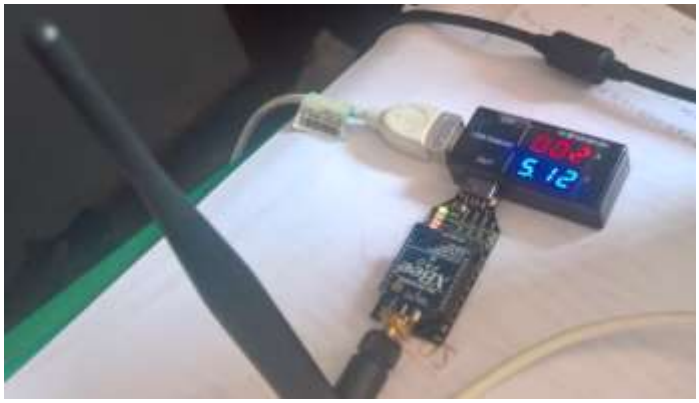

Figura 2-3. Medición en el Nodo Gateway

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.1 Medición en el Gateway en una distancia de cien metros

3.2.1.1 Algoritmo RSA en una distancia de cien metros (Primer Día).

En la Tabla 2-3, Tabla 3-3 y Tabla 4-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 2-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	2192
8:08:00	0,05	30046
8:12:00	0,04	12856
8:16:00	0,05	39466
8:20:00	0,07	72549
8:24:00	0,05	100845
8:28:00	0,04	158245
8:32:00	0,05	172965
8:36:00	0,05	220123
8:40:00	0,05	278441
8:44:00	0,05	339812
8:48:00	0,05	378451
8:52:00	0,04	428961
8:56:00	0,05	486321
9:00:00	0,05	501247

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 3-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,04	503002
9:08:00	0,04	540391
9:12:00	0,04	542575
9:16:00	0,05	568896
9:20:00	0,04	575943
9:24:00	0,05	577646
9:28:00	0,04	687383
9:32:00	0,07	701897
9:36:00	0,05	719978
9:40:00	0,05	721779
9:44:00	0,05	735171
9:48:00	0,05	751416
9:52:00	0,04	752447
9:56:00	0,04	802092
10:00:00	0,05	804541

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 4-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	810241
10:08:00	0,05	812752
10:12:00	0,04	815001
10:16:00	0,05	818302
10:20:00	0,04	842012
10:24:00	0,05	845178
10:28:00	0,04	849478
10:32:00	0,02	878147
10:36:00	0,05	890475
10:40:00	0,05	897635
10:44:00	0,05	901852
10:48:00	0,05	914785
10:52:00	0,04	920147
10:56:00	0,07	922578
11:00:00	0,05	925741
11:04:00	0,05	930558
11:08:00	0,05	932105
11:12:00	0,07	938004
11:16:00	0,05	940114
11:20:00	0,07	946789

Fuente: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 5-3, Tabla 6-3 y Tabla 7-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 5-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
12:04:00	0,04	2200
12:08:00	0,07	32467
12:12:00	0,04	34856
12:16:00	0,05	40126
12:20:00	0,04	74019
12:24:00	0,05	103785
12:28:00	0,05	159478
12:32:00	0,05	173451
12:36:00	0,05	227013
12:40:00	0,04	279154
12:44:00	0,07	340814
12:48:00	0,05	379741
12:52:00	0,05	429231
12:56:00	0,05	488441
13:00:00	0,05	503485

Fuente: Andrés Solís, Ítalo Parreño, 2019

Tabla 6-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
13:04:00	0,04	503725
13:08:00	0,05	540785
13:12:00	0,04	544887
13:16:00	0,05	569632
13:20:00	0,02	570102
13:24:00	0,05	574523
13:28:00	0,07	689658
13:32:00	0,07	701789
13:36:00	0,05	718751
13:40:00	0,05	721003
13:44:00	0,05	735753
13:48:00	0,05	751951
13:52:00	0,04	752741
13:56:00	0,04	802788
14:00:00	0,05	804963

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 7-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
14:04:00	0,04	808951
14:08:00	0,05	812459
14:12:00	0,04	815123
14:16:00	0,05	817596
14:20:00	0,04	820520
14:24:00	0,05	829632
14:28:00	0,04	835654
14:32:00	0,02	840521
14:36:00	0,05	845987
14:40:00	0,05	860235
14:44:00	0,05	902123
14:48:00	0,05	910258
14:52:00	0,07	912475
14:56:00	0,07	917854
15:00:00	0,05	920741
15:04:00	0,05	922784
15:08:00	0,05	935102
15:12:00	0,07	940215
15:16:00	0,05	960148
15:20:00	0,07	978520

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 8-3, Tabla 9-3 y Tabla 10-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 8-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
16:04:00	0,07	2180
16:08:00	0,06	30055
16:12:00	0,06	129811
16:16:00	0,07	39524
20:20:00	0,05	72678
16:24:00	0,05	100100
16:28:00	0,04	158932
16:32:00	0,04	172621
16:36:00	0,05	222450
16:40:00	0,05	278441
16:44:00	0,04	334789
16:48:00	0,04	378603
16:52:00	0,05	429003
16:56:00	0,06	486451
17:00:00	0,06	501789

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 9-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
17:04:00	0,07	502972
17:08:00	0,04	504125
17:12:00	0,04	504789
17:16:00	0,07	514753
17:20:00	0,06	525698
17:24:00	0,06	532125
17:28:00	0,07	541257
17:32:00	0,06	621752
17:36:00	0,05	640415
17:40:00	0,04	682145
17:44:00	0,07	701458
17:48:00	0,06	708596
17:52:00	0,04	712478
17:56:00	0,05	715425
2200:00	0,04	725852

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 10-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
18:04:00	0,05	800214
18:08:00	0,07	801741
18:12:00	0,07	808596
18:16:00	0,06	812547
18:20:00	0,05	820302
18:24:00	0,06	827851
18:28:00	0,05	835265
18:32:00	0,06	841574
18:36:00	0,03	845558
18:40:00	0,04	856321
18:44:00	0,02	865201
18:48:00	0,06	878963
18:52:00	0,07	895203
18:56:00	0,06	902145
19:00:00	0,02	910425
19:04:00	0,07	915478
19:08:00	0,02	920654
19:12:00	0,07	922578
19:16:00	0,03	930125
19:20:00	0,07	945879

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 11-3, Tabla 12-3 y Tabla 13-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 11-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
20:04:00	0,05	2270
20:08:00	0,04	30096
20:12:00	0,04	12917
20:16:00	0,05	39541
20:20:00	0,05	72648
20:24:00	0,05	100927
20:28:00	0,04	158337
20:32:00	0,07	173024
20:36:00	0,05	220165
20:40:00	0,04	278500
20:44:00	0,04	339877
20:48:00	0,05	378529
20:52:00	0,04	429056
20:56:00	0,05	486383
21:00:00	0,05	501346

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 12-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
21:04:00	0,04	504212
21:08:00	0,05	510235
21:12:00	0,04	515654
21:16:00	0,05	520221
21:20:00	0,04	525454
21:24:00	0,07	532102
21:28:00	0,04	536214
21:32:00	0,05	550241
21:36:00	0,05	554785
21:40:00	0,05	561203
21:44:00	0,05	563201
21:48:00	0,04	598674
21:52:00	0,04	611032
21:56:00	0,04	625458
22:00:00	0,05	630214

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 13-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Corriente (A)	Bytes Rx
22:04:00	0,04	632104
22:08:00	0,04	642587
22:12:00	0,05	651458
22:16:00	0,05	666789
22:20:00	0,04	682478
22:24:00	0,02	702456
22:28:00	0,04	715423
22:32:00	0,04	725853
22:36:00	0,04	763548
22:40:00	0,05	775968
22:44:00	0,04	791300
22:48:00	0,05	802536
22:52:00	0,07	815456
22:56:00	0,05	830296
23:00:00	0,05	842554
23:04:00	0,07	860756
23:08:00	0,05	878952
23:12:00	0,04	903478
23:16:00	0,07	912554
23:20:00	0,05	935668

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.1.2 Algoritmo AES 256 en una distancia de cien metros (Segundo Día).

En la Tabla 14-3, Tabla 15-3 y Tabla 16-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 14-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	2291
8:08:00	0,04	24290
8:12:00	0,04	74026
8:16:00	0,04	124004
8:20:00	0,04	189119
8:24:00	0,05	225712
8:28:00	0,04	291454
8:32:00	0,04	328830
8:36:00	0,04	389334
8:40:00	0,04	445333
8:44:00	0,04	429660
8:48:00	0,04	528523
8:52:00	0,05	544869
8:56:00	0,04	547212
9:00:00	0,04	595460

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 15-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,04	598120
9:08:00	0,04	603258
9:12:00	0,04	621586
9:16:00	0,04	675896
9:20:00	0,04	702548
9:24:00	0,05	720896
9:28:00	0,04	760555
9:32:00	0,04	801452
9:36:00	0,04	820145
9:40:00	0,04	832569
9:44:00	0,04	840225
9:48:00	0,04	849785
9:52:00	0,05	860205
9:56:00	0,04	865789
10:00:00	0,04	870214

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 16-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	891458
10:08:00	0,04	902777
10:12:00	0,04	915245
10:16:00	0,04	917852
10:20:00	0,04	921630
10:24:00	0,05	922568
10:28:00	0,04	925789
10:32:00	0,04	935201
10:36:00	0,04	941525
10:40:00	0,04	947852
10:44:00	0,04	958741
10:48:00	0,04	968596
10:52:00	0,05	972563
10:56:00	0,04	978593
11:00:00	0,04	1000102
11:04:00	0,04	1004789
11:08:00	0,04	1010425
11:12:00	0,04	1025789
11:16:00	0,05	1031456
11:20:00	0,05	1048596

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 17-3, Tabla 18-3 y Tabla 19-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 17-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
12:04:00	0,04	2278
12:08:00	0,04	22002
12:12:00	0,04	73126
12:16:00	0,04	123704
12:20:00	0,04	189349
12:24:00	0,05	225895
12:28:00	0,04	291714
12:32:00	0,04	328951
12:36:00	0,04	389102
12:40:00	0,04	445648
12:44:00	0,04	429784
12:48:00	0,04	528410
12:52:00	0,05	545819
12:56:00	0,04	547654
13:00:00	0,04	595752

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 18-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
13:04:00	0,04	598789
13:08:00	0,04	603457
13:12:00	0,04	622125
13:16:00	0,04	676987
13:20:00	0,02	704789
13:24:00	0,05	722569
13:28:00	0,04	761458
13:32:00	0,04	803520
13:36:00	0,04	822147
13:40:00	0,04	834589
13:44:00	0,04	846325
13:48:00	0,04	849002
13:52:00	0,05	86325
13:56:00	0,04	866874
14:00:00	0,04	872458

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 19-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
14:04:00	0,04	892468
14:08:00	0,04	904747
14:12:00	0,04	914005
14:16:00	0,04	916805
14:20:00	0,04	922610
14:24:00	0,05	923508
14:28:00	0,04	928289
14:32:00	0,05	936211
14:36:00	0,04	942515
14:40:00	0,04	948152
14:44:00	0,04	959007
14:48:00	0,04	965516
14:52:00	0,05	972503
14:56:00	0,04	978113
15:00:00	0,05	1000192
15:04:00	0,04	1004709
15:08:00	0,04	1010445
15:12:00	0,04	1025749
15:16:00	0,05	1031742
15:20:00	0,05	1049005

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 20-3, Tabla 21-3 y Tabla 22-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 20-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
16:04:00	0,04	2347
16:08:00	0,05	24198
16:12:00	0,05	74129
16:16:00	0,04	123474
20:20:00	0,04	188479
16:24:00	0,05	226472
16:28:00	0,05	292474
16:32:00	0,04	327450
16:36:00	0,04	388794
16:40:00	0,04	444633
16:44:00	0,05	428460
16:48:00	0,04	525473
16:52:00	0,05	546019
16:56:00	0,05	546472
17:00:00	0,05	596007

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 21-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
17:04:00	0,05	597136
17:08:00	0,05	598721
17:12:00	0,05	604557
17:16:00	0,05	624825
17:20:00	0,04	677017
17:24:00	0,04	706259
17:28:00	0,04	723669
17:32:00	0,04	762258
17:36:00	0,05	804220
17:40:00	0,05	824117
17:44:00	0,05	834001
17:48:00	0,05	847305
17:52:00	0,04	849012
17:56:00	0,05	864200
2200:00	0,04	871254

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 22-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
18:04:00	0,04	893408
18:08:00	0,05	905707
18:12:00	0,05	913015
18:16:00	0,04	915205
18:20:00	0,04	921110
18:24:00	0,05	924208
18:28:00	0,04	927209
18:32:00	0,05	936211
18:36:00	0,04	941505
18:40:00	0,04	948002
18:44:00	0,05	958005
18:48:00	0,04	965116
18:52:00	0,04	970603
18:56:00	0,04	977003
19:00:00	0,04	1000102
19:04:00	0,05	1004779
19:08:00	0,04	1010145
19:12:00	0,04	1025849
19:16:00	0,04	1031942
19:20:00	0,05	1059077

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 23-3, Tabla 24-3 y Tabla 25-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 23-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
20:04:00	0,04	2339
20:08:00	0,04	24381
20:12:00	0,04	74098
20:16:00	0,05	124081
20:20:00	0,05	189163
20:24:00	0,04	225762
20:28:00	0,05	291520
20:32:00	0,04	328904
20:36:00	0,05	389404
20:40:00	0,05	445373
20:44:00	0,04	429719
20:48:00	0,04	528583
20:52:00	0,04	544927
20:56:00	0,05	547283
21:00:00	0,05	595511

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 24-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
21:04:00	0,04	599082
21:08:00	0,04	600136
21:12:00	0,05	603721
21:16:00	0,04	608507
21:20:00	0,04	624825
21:24:00	0,04	670027
21:28:00	0,04	705219
21:32:00	0,05	723669
21:36:00	0,04	763558
21:40:00	0,04	806320
21:44:00	0,05	825717
21:48:00	0,04	835001
21:52:00	0,04	848405
21:56:00	0,05	855112
22:00:00	0,04	863270

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 25-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	Corriente (A)	Bytes Rx
22:04:00	0,05	892428
22:08:00	0,04	906717
22:12:00	0,04	913051
22:16:00	0,04	915215
22:20:00	0,05	920120
22:24:00	0,04	924278
22:28:00	0,04	928889
22:32:00	0,04	936200
22:36:00	0,05	942665
22:40:00	0,04	948669
22:44:00	0,04	958742
22:48:00	0,05	966987
22:52:00	0,04	970123
22:56:00	0,04	977008
23:00:00	0,04	1000174
23:04:00	0,04	1004669
23:08:00	0,04	1010885
23:12:00	0,04	1025779
23:16:00	0,05	1031992
23:20:00	0,05	1079666

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.1.3 Algoritmo AES 192 en una distancia de cien metros (Tercer Día).

En la Tabla 26-3, Tabla 27-3 y Tabla 28-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 26-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	1580
8:08:00	0,05	2796
8:12:00	0,04	18423
8:16:00	0,05	22823
8:20:00	0,04	41047
8:24:00	0,04	67103
8:28:00	0,04	86343
8:32:00	0,04	99739
8:36:00	0,05	126187
8:40:00	0,05	172803
8:44:00	0,04	190205
8:48:00	0,05	220797
8:52:00	0,04	249066
8:56:00	0,02	283310
9:00:00	0,04	300813

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 27-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,04	305914
9:08:00	0,05	315222
9:12:00	0,04	335687
9:16:00	0,05	387521
9:20:00	0,04	402551
9:24:00	0,04	415236
9:28:00	0,04	421536
9:32:00	0,04	437458
9:36:00	0,05	440594
9:40:00	0,05	442152
9:44:00	0,04	445871
9:48:00	0,05	450325
9:52:00	0,04	452102
9:56:00	0,02	455789
10:00:00	0,04	459862

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 28-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	460120
10:08:00	0,05	462589
10:12:00	0,04	472510
10:16:00	0,05	474520
10:20:00	0,04	476227
10:24:00	0,04	480563
10:28:00	0,04	482562
10:32:00	0,04	485785
10:36:00	0,05	488571
10:40:00	0,05	490112
10:44:00	0,04	492568
10:48:00	0,05	494785
10:52:00	0,04	496785
10:56:00	0,02	498002
11:00:00	0,04	500236
11:04:00	0,05	502369
11:08:00	0,04	504785
11:12:00	0,04	507895
11:16:00	0,04	510235
11:20:00	0,05	515230

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 29-3, Tabla 30-3 y Tabla 31-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 29-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
12:04:00	0,04	1270
12:08:00	0,05	2686
12:12:00	0,04	18423
12:16:00	0,05	21403
12:20:00	0,04	41302
12:24:00	0,04	67103
12:28:00	0,04	86774
12:32:00	0,04	99839
12:36:00	0,05	126857
12:40:00	0,05	172893
12:44:00	0,04	190305
12:48:00	0,05	220807
12:52:00	0,04	249145
12:56:00	0,02	283710
13:00:00	0,04	300903

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 30-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
13:04:00	0,04	305925
13:08:00	0,05	307900
13:12:00	0,04	312592
13:16:00	0,05	315025
13:20:00	0,04	317115
13:24:00	0,05	319110
13:28:00	0,04	321584
13:32:00	0,04	333078
13:36:00	0,05	336987
13:40:00	0,05	333875
13:44:00	0,04	335325
13:48:00	0,05	345115
13:52:00	0,04	368785
13:56:00	0,02	375025
14:00:00	0,04	389510

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 31-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
14:04:00	0,04	400210
14:08:00	0,05	414500
14:12:00	0,04	425510
14:16:00	0,05	429650
14:20:00	0,04	435207
14:24:00	0,04	440213
14:28:00	0,04	442562
14:32:00	0,04	448785
14:36:00	0,05	452571
14:40:00	0,05	459012
14:44:00	0,04	464568
14:48:00	0,05	466785
14:52:00	0,05	468785
14:56:00	0,02	472002
15:00:00	0,04	487236
15:04:00	0,05	492369
15:08:00	0,04	498785
15:12:00	0,04	500895
15:16:00	0,04	505235
15:20:00	0,05	508230

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 32-3, Tabla 33-3 y Tabla 34-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 32-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
16:04:00	0,03	1719
16:08:00	0,05	2935
16:12:00	0,05	18562
16:16:00	0,05	22962
16:20:00	0,04	41186
16:24:00	0,04	67242
16:28:00	0,05	86482
16:32:00	0,02	99878
16:36:00	0,04	126326
16:40:00	0,05	172942
16:44:00	0,04	190344
16:48:00	0,03	220936
16:52:00	0,04	249205
16:56:00	0,05	283449
17:00:00	0,04	300952

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 33-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
17:04:00	0,04	305925
17:08:00	0,04	307102
17:12:00	0,03	311002
17:16:00	0,04	313147
17:20:00	0,04	319753
17:24:00	0,05	320487
17:28:00	0,05	322741
17:32:00	0,04	329852
17:36:00	0,05	334721
17:40:00	0,02	337963
17:44:00	0,04	340325
17:48:00	0,03	342115
17:52:00	0,04	348789
17:56:00	0,04	368741
18:00:00	0,05	375698

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 34-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
18:04:00	0,04	402159
18:08:00	0,04	410256
18:12:00	0,05	415274
18:16:00	0,05	419854
18:20:00	0,03	422563
18:24:00	0,05	428753
18:28:00	0,04	433698
18:32:00	0,05	438741
18:36:00	0,03	441255
18:40:00	0,05	449632
18:44:00	0,02	451247
18:48:00	0,04	456952
18:52:00	0,05	459852
18:56:00	0,03	464521
19:00:00	0,04	472589
19:04:00	0,04	482520
19:08:00	0,05	487693
19:12:00	0,04	458789
19:16:00	0,05	465258
19:20:00	0,05	475896

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 35-3, Tabla 36-3 y Tabla 37-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 35-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
20:04:00	0,04	1594
20:08:00	0,04	2894
20:12:00	0,05	18494
20:16:00	0,05	23770
20:20:00	0,04	41777
20:24:00	0,04	67137
20:28:00	0,04	86798
20:32:00	0,05	100410
20:36:00	0,04	126872
20:40:00	0,05	173530
20:44:00	0,02	191221
20:48:00	0,05	221742
20:52:00	0,05	249705
20:56:00	0,04	283730
21:00:00	0,04	301134

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 36-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
21:04:00	0,04	306015
21:08:00	0,04	312578
21:12:00	0,04	322785
21:16:00	0,05	335892
21:20:00	0,05	337896
21:24:00	0,04	342589
21:28:00	0,02	345698
21:32:00	0,04	352147
21:36:00	0,05	361258
21:40:00	0,04	367852
21:44:00	0,04	375842
21:48:00	0,05	381259
21:52:00	0,04	389751
21:56:00	0,05	401259
22:00:00	0,04	408965

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 37-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	Corriente (A)	Bytes Rx
22:04:00	0,04	415236
22:08:00	0,04	420582
22:12:00	0,05	432598
22:16:00	0,05	441785
22:20:00	0,04	452185
22:24:00	0,04	461241
22:28:00	0,04	469862
22:32:00	0,04	475852
22:36:00	0,05	483654
22:40:00	0,02	493652
22:44:00	0,04	498511
22:48:00	0,05	502147
22:52:00	0,05	505210
22:56:00	0,04	506987
23:00:00	0,04	508741
23:04:00	0,04	512425
23:08:00	0,05	515478
23:12:00	0,04	520852
23:16:00	0,05	524852
23:20:00	0,05	530206

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.1.4 Algoritmo AES 128 en una distancia de cien metros (Cuarto Día).

En la Tabla 38-3, Tabla 39-3 y Tabla 40-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 38-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	2800
8:08:00	0,05	5214
8:12:00	0,04	6772
8:16:00	0,05	8544
8:20:00	0,04	42221
8:24:00	0,04	58361
8:28:00	0,04	75609
8:32:00	0,04	88443
8:36:00	0,04	106545
8:40:00	0,04	131048
8:44:00	0,04	160227
8:48:00	0,04	178663
8:52:00	0,04	210211
8:56:00	0,04	229700
9:00:00	0,04	256414

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 39-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,04	257474
9:08:00	0,05	261254
9:12:00	0,04	271452
9:16:00	0,05	273654
9:20:00	0,04	277805
9:24:00	0,04	279862
9:28:00	0,04	304785
9:32:00	0,04	313666
9:36:00	0,04	325896
9:40:00	0,04	333654
9:44:00	0,04	345510
9:48:00	0,04	351201
9:52:00	0,04	356890
9:56:00	0,04	362501
10:00:00	0,04	369842

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 40-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	372451
10:08:00	0,05	380254
10:12:00	0,04	385421
10:16:00	0,05	387555
10:20:00	0,04	390514
10:24:00	0,04	394578
10:28:00	0,04	398753
10:32:00	0,04	400222
10:36:00	0,04	415203
10:40:00	0,04	421547
10:44:00	0,04	427521
10:48:00	0,04	432587
10:52:00	0,04	437895
10:56:00	0,04	442559
11:00:00	0,04	449852
11:04:00	0,04	453201
11:08:00	0,05	458147
11:12:00	0,04	462875
11:16:00	0,04	472589
11:20:00	0,04	477012

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 41-3, Tabla 42-3 y Tabla 43-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 41-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
12:04:00	0,04	2700
12:08:00	0,05	5200
12:12:00	0,04	6701
12:16:00	0,05	8504
12:20:00	0,04	42741
12:24:00	0,04	58412
12:28:00	0,04	75779
12:32:00	0,04	88401
12:36:00	0,04	106874
12:40:00	0,04	131753
12:44:00	0,04	160742
12:48:00	0,04	178012
12:52:00	0,04	210365
12:56:00	0,04	229652
13:00:00	0,04	256001

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 42-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
13:04:00	0,04	259626
13:08:00	0,05	265851
13:12:00	0,04	274589
13:16:00	0,05	281502
13:20:00	0,04	288630
13:24:00	0,04	290509
13:28:00	0,04	295874
13:32:00	0,04	302450
13:36:00	0,02	309541
13:40:00	0,04	313764
13:44:00	0,04	320512
13:48:00	0,04	328601
13:52:00	0,04	333668
13:56:00	0,04	339601
14:00:00	0,04	342111

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 43-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
14:04:00	0,04	349012
14:08:00	0,05	356999
14:12:00	0,04	362511
14:16:00	0,05	366933
14:20:00	0,04	375200
14:24:00	0,05	380245
14:28:00	0,04	389541
14:32:00	0,04	392003
14:36:00	0,04	398999
14:40:00	0,04	400257
14:44:00	0,04	409105
14:48:00	0,04	410200
14:52:00	0,04	417500
14:56:00	0,04	424369
15:00:00	0,04	433665
15:04:00	0,04	439006
15:08:00	0,05	441220
15:12:00	0,04	449008
15:16:00	0,04	453210
15:20:00	0,04	462009

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 44-3, Tabla 45-3 y Tabla 46-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 44-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
16:04:00	0,04	2749
16:08:00	0,05	5196
16:12:00	0,05	6496
16:16:00	0,04	8373
16:20:00	0,05	43478
16:24:00	0,05	58276
16:28:00	0,04	76039
16:32:00	0,04	88279
16:36:00	0,04	107439
16:40:00	0,05	130978
16:44:00	0,04	160347
16:48:00	0,04	177625
16:52:00	0,05	210347
16:56:00	0,04	228736
17:00:00	0,05	257028

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 45-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
17:04:00	0,04	254116
17:08:00	0,04	266001
17:12:00	0,05	273669
17:16:00	0,04	280632
17:20:00	0,05	287770
17:24:00	0,05	292119
17:28:00	0,04	296784
17:32:00	0,04	303660
17:36:00	0,04	309666
17:40:00	0,05	314784
17:44:00	0,05	322112
17:48:00	0,04	327991
17:52:00	0,05	334678
17:56:00	0,04	338678
18:00:00	0,05	342333

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 46-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
18:04:00	0,05	348812
18:08:00	0,04	354512
18:12:00	0,05	364444
18:16:00	0,04	369632
18:20:00	0,05	374753
18:24:00	0,05	380952
18:28:00	0,04	388962
18:32:00	0,04	391003
18:36:00	0,04	399639
18:40:00	0,05	400123
18:44:00	0,05	407541
18:48:00	0,04	410200
18:52:00	0,04	419850
18:56:00	0,04	424369
19:00:00	0,04	435775
19:04:00	0,05	439886
19:08:00	0,04	443990
19:12:00	0,04	449228
19:16:00	0,04	454770
19:20:00	0,04	464779

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 47-3, Tabla 48-3 y Tabla 49-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 47-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
20:04:00	0,05	2836
20:08:00	0,05	5241
20:12:00	0,04	6851
20:16:00	0,04	8636
20:20:00	0,04	42248
20:24:00	0,05	59039
20:28:00	0,04	76457
20:32:00	0,05	88810
20:36:00	0,04	107528
20:40:00	0,05	131399
20:44:00	0,04	160845
20:48:00	0,05	179600
20:52:00	0,04	210423
20:56:00	0,05	230645
21:00:00	0,04	256438

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 48-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
21:04:00	0,05	254427
21:08:00	0,04	267852
21:12:00	0,04	273753
21:16:00	0,05	280951
21:20:00	0,05	287258
21:24:00	0,04	292741
21:28:00	0,04	296125
21:32:00	0,05	303325
21:36:00	0,04	309785
21:40:00	0,04	314854
21:44:00	0,05	322965
21:48:00	0,04	327457
21:52:00	0,04	334785
21:56:00	0,04	338857
22:00:00	0,04	346985

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 49-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	Corriente (A)	Bytes Rx
22:04:00	0,04	3488014
22:08:00	0,05	354951
22:12:00	0,05	364753
22:16:00	0,04	369854
22:20:00	0,04	374784
22:24:00	0,04	380985
22:28:00	0,05	388452
22:32:00	0,04	391652
22:36:00	0,04	399412
22:40:00	0,05	400368
22:44:00	0,04	407987
22:48:00	0,05	410778
22:52:00	0,04	419852
22:56:00	0,04	424957
23:00:00	0,05	435153
23:04:00	0,04	439751
23:08:00	0,04	443953
23:12:00	0,04	449824
23:16:00	0,05	454971
23:20:00	0,04	464938

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.1.5 Texto Plano en una distancia de cien metros (Quinto Día).

En la Tabla 50-3, Tabla 51-3 y Tabla 52-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 50-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	2894
8:08:00	0,05	10114
8:12:00	0,04	12856
8:16:00	0,05	39466
8:20:00	0,04	72549
8:24:00	0,05	97626
8:28:00	0,04	100841
8:32:00	0,02	128830
8:36:00	0,05	158241
8:40:00	0,05	172803
8:44:00	0,04	190205
8:48:00	0,05	220797
8:52:00	0,04	249066
8:56:00	0,02	283310
9:00:00	0,04	300813

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 51-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,04	303427
9:08:00	0,05	306851
9:12:00	0,04	310478
9:16:00	0,05	318965
9:20:00	0,04	321789
9:24:00	0,05	327895
9:28:00	0,04	332578
9:32:00	0,02	337895
9:36:00	0,05	341205
9:40:00	0,05	349875
9:44:00	0,04	353260
9:48:00	0,05	359806
9:52:00	0,04	362048
9:56:00	0,02	366987
10:00:00	0,04	369845

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 52-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	370485
10:08:00	0,05	374561
10:12:00	0,04	378756
10:16:00	0,05	401654
10:20:00	0,04	405753
10:24:00	0,05	410952
10:28:00	0,04	417148
10:32:00	0,02	422125
10:36:00	0,05	429458
10:40:00	0,05	432751
10:44:00	0,04	438954
10:48:00	0,05	442857
10:52:00	0,04	448632
10:56:00	0,02	451745
11:00:00	0,04	458985
11:04:00	0,04	461325
11:08:00	0,04	469856
11:12:00	0,04	472952
11:16:00	0,04	475012
11:20:00	0,02	479026

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 53-3, Tabla 54-3 y Tabla 55-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 53-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
12:04:00	0,04	2752
12:08:00	0,05	10221
12:12:00	0,04	12741
12:16:00	0,05	39902
12:20:00	0,04	72746
12:24:00	0,02	97963
12:28:00	0,04	100300
12:32:00	0,02	128441
12:36:00	0,05	158241
12:40:00	0,05	172803
12:44:00	0,04	190325
12:48:00	0,05	220707
12:52:00	0,04	249060
12:56:00	0,02	283410
13:00:00	0,04	300903

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 54-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
13:04:00	0,04	303351
13:08:00	0,05	312457
13:12:00	0,04	318952
13:16:00	0,02	326874
13:20:00	0,04	332001
13:24:00	0,05	341206
13:28:00	0,04	348521
13:32:00	0,02	351206
13:36:00	0,05	359842
13:40:00	0,05	362035
13:44:00	0,04	369000
13:48:00	0,05	374512
13:52:00	0,04	376521
13:56:00	0,02	381203
14:00:00	0,04	388951

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 55-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
14:04:00	0,04	390485
14:08:00	0,02	394561
14:12:00	0,04	398756
14:16:00	0,05	401245
14:20:00	0,04	405698
14:24:00	0,05	410269
14:28:00	0,04	417895
14:32:00	0,04	422598
14:36:00	0,05	429875
14:40:00	0,02	432014
14:44:00	0,04	438521
14:48:00	0,05	442857
14:52:00	0,04	448632
14:56:00	0,02	451206
15:00:00	0,04	458951
15:04:00	0,04	461257
15:08:00	0,04	469654
15:12:00	0,04	472510
15:16:00	0,04	475891
15:20:00	0,04	479851

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 56-3, Tabla 57-3 y Tabla 58-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 56-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
16:04:00	0,05	2843
16:08:00	0,04	10463
16:12:00	0,04	13205
16:16:00	0,04	39815
16:20:00	0,02	72898
16:24:00	0,04	97975
16:28:00	0,04	101190
16:32:00	0,05	129179
16:36:00	0,05	159290
16:40:00	0,02	172152
16:44:00	0,05	191054
16:48:00	0,04	221246
16:52:00	0,03	249415
16:56:00	0,05	283659
17:00:00	0,05	301162

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 57-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
17:04:00	0,05	302451
17:08:00	0,04	311787
17:12:00	0,04	319752
17:16:00	0,05	325004
17:20:00	0,04	331741
17:24:00	0,02	340365
17:28:00	0,03	347661
17:32:00	0,05	352576
17:36:00	0,05	358662
17:40:00	0,04	361475
17:44:00	0,02	370890
17:48:00	0,04	374662
17:52:00	0,03	377591
17:56:00	0,04	382569
18:00:00	0,05	388771

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 58-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
18:04:00	0,05	390201
18:08:00	0,03	395962
18:12:00	0,05	399875
18:16:00	0,02	401302
18:20:00	0,05	405887
18:24:00	0,03	410784
18:28:00	0,05	416954
18:32:00	0,04	422114
18:36:00	0,03	429789
18:40:00	0,04	432009
18:44:00	0,05	438785
18:48:00	0,04	442960
18:52:00	0,03	448874
18:56:00	0,05	451906
19:00:00	0,05	458332
19:04:00	0,05	461447
19:08:00	0,04	469558
19:12:00	0,02	472954
19:16:00	0,05	475666
19:20:00	0,04	478877

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 59-3, Tabla 60-3 y Tabla 61-3; se detallan los valores de corriente y bytes recibidos de los cinco nodos sensores durante las tres horas con veinte minutos.

Tabla 59-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
8:04:00	0,04	2962
8:08:00	0,04	10151
8:12:00	0,05	12914
8:16:00	0,05	39760
8:20:00	0,05	73270
8:24:00	0,04	98997
8:28:00	0,04	102233
8:32:00	0,04	129575
8:36:00	0,05	159575
8:40:00	0,02	173520
8:44:00	0,04	190763
8:48:00	0,02	221585
8:52:00	0,04	250176
8:56:00	0,05	283878
9:00:00	0,04	301018

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 60-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
9:04:00	0,05	303401
9:08:00	0,05	318787
9:12:00	0,04	322752
9:16:00	0,02	329004
9:20:00	0,05	333741
9:24:00	0,05	340365
9:28:00	0,04	347661
9:32:00	0,04	354576
9:36:00	0,05	358222
9:40:00	0,05	361885
9:44:00	0,04	370990
9:48:00	0,05	372332
9:52:00	0,04	377666
9:56:00	0,02	382458
10:00:00	0,04	388751

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 61-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	Corriente (A)	Bytes Rx
10:04:00	0,04	390147
10:08:00	0,05	395785
10:12:00	0,05	399965
10:16:00	0,05	402358
10:20:00	0,04	407895
10:24:00	0,02	410754
10:28:00	0,04	417854
10:32:00	0,05	422741
10:36:00	0,05	428520
10:40:00	0,04	432000
10:44:00	0,04	439632
10:48:00	0,02	447569
10:52:00	0,04	451478
10:56:00	0,05	454901
11:00:00	0,04	459874
11:04:00	0,04	468555
11:08:00	0,02	473288
11:12:00	0,04	479655
11:16:00	0,05	481775
11:20:00	0,04	487632

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.2.2 Comparación de Mediciones en el *Gateway*

3.2.2.1 Comparación de Valores de Corriente en una distancia de 100 metros

Tabla 62-3. Datos Promedio De los Algoritmos Realizados en 100 metros

Algoritmo	Valor de Media de Corriente	Valor de Media de Bytes Rx
Texto Plano	0,0402 A	318986
AES 128	0,0357 A	302703
AES 192	0,0420 A	333332
AES 256	0,0429 A	700506
RSA	0,0476 A	593401

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En el Gráfico 1-3 se observa una comparativa entre las medias obtenidas de los cincuenta datos en los diferentes algoritmos comparados con texto plano. Se puede observar que el algoritmo RSA registra en cuanto a corriente un valor de 0,0476 A, mientras el algoritmo AES 192 registra un valor en corriente de 0,0420 A, el algoritmo AES 128 registra un valor en corriente de 0,0357 A y el algoritmo AES 256 registra un valor en corriente de 0.0429 A. Texto Plano registra un valor en corriente de 0.0402 A.

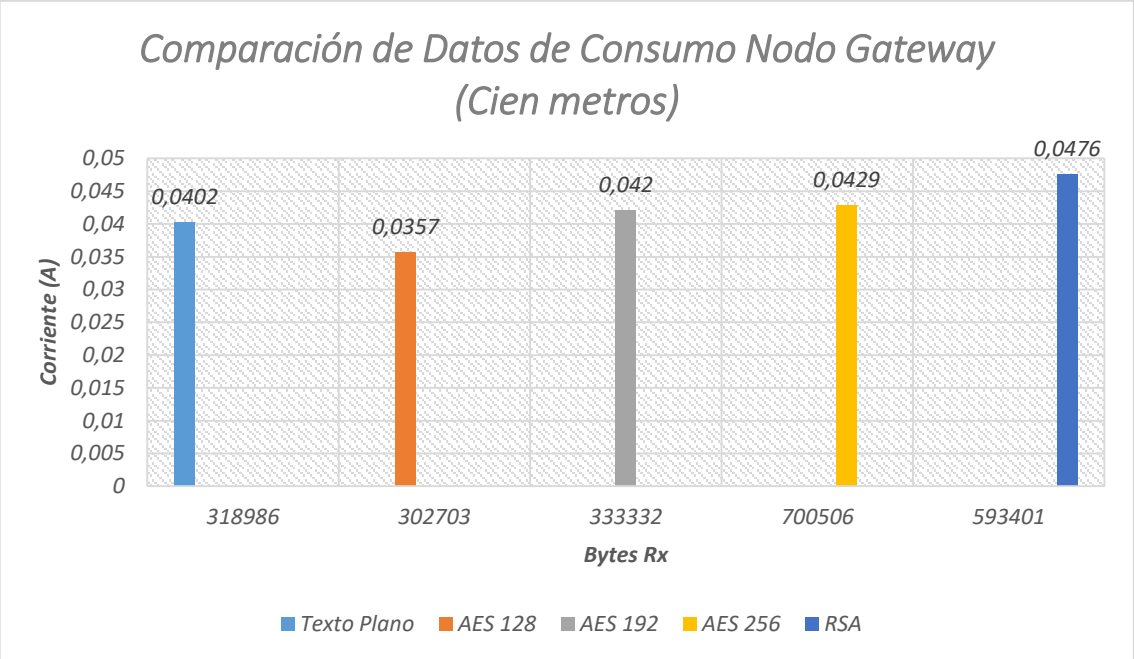

Gráfico 1-3. Comparación de Datos de Consumo en el Gateway (Cien metros)

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3 Mediciones en el Nodo Sensor

3.3.1 Prueba de Medición a 100 metros

A continuación, se mostrarán los resultados obtenidos al desplegar el escenario en una distancia de cien metros entre los nodos sensores y el *gateway*, utilizando los algorimos AES 128, AES 192, AES 254 y RSA, además del texto plano para asi poder compararlos con este último y obtener el consumo que presentan dichos algoritmos. Para las mediciones utilizamos dos dispositivos, un multímetro genérico Serie 830, un multímetro RadioShack. En las Figura 3-3 se observa como el Multímetro Genérico está conectado al Nodo Sensor, en el momento de enviar los datos.

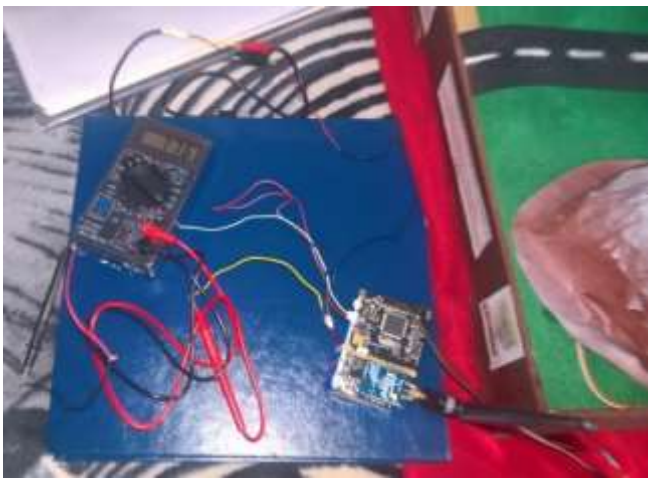

Figura 3-3. Medida en el Nodo Sensor

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En las Figura 4-3 se observa como el multímetro de marca RadioShack está conectado al Nodo Sensor, en el momento de enviar los datos

Figura 4-3. Medida en el Nodo Sensor

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3.1.1 Prueba de Medición a 100 metros con el algoritmo RSA (Primer Día)

En la Tabla 63-3, Tabla 64-3 y Tabla 65-3 se detallan los valores de corriente, realizadas con el algoritmo RSA, el máximo tamaño de transmisión es de 96 bytes.

Tabla 63-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
8:04	81,2	83
8:08	82,4	82,8
8:12	80,9	82,9
8:16	80,7	80,5
8:20	81,6	81
8:24	82	80,9
8:28	82,2	82,3
8:32	83,1	82,5
8:36	80,8	81,6
8:40	81,2	80,8
8:44	82,2	81,7
8:48	81,1	80,9
8:52	82,3	81
8:56	82,5	82,6
9:00	82,4	81,7

Realizado por: Andrés Solís, Ítalo Parreño, 2019+

Tabla 64-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
9:04	81	80,8
9:08	81,6	82,1
9:12	81,8	81,3
9:16	81,6	80,5
9:20	82,6	81,6
9:24	80,6	81,3
9:28	82,7	80,5
9:32	81,2	83
9:36	81	82
9:40	81,1	81,2
9:44	82,6	82,9
9:48	81,5	80,7
9:52	80,6	82
9:56	81,3	80,7
10:00	82,9	81,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 65-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
10:04	82,1	80,4
10:08	80,6	80,4
10:12	80,6	81,6
10:16	81,7	81,9
10:20	81,3	80,8
10:24	82,9	82
10:28	81,5	83
10:32	81,9	82
10:36	80,5	80,6
10:40	81,8	83
10:44	80,5	82,5
10:48	81,5	82,3
10:52	82,3	82,7
10:56	82,7	82,8
11:00	81,7	80,8
11:04	81,6	81,4
11:08	81,1	82
11:12	80,8	83
11:16	80,6	82,5
11:20	82,3	81,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 66-3, Tabla 67-3 y Tabla 68-3 se detallan los valores de corriente, algoritmo RSA.

Tabla 66-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Multímetro Genérico (mA)	Multímetro RadioShack (mA)
12:04	82,5	81,8
12:08	82,8	80,6
12:12	82,7	81,5
12:16	82,1	82,1
12:20	81,2	80,6
12:24	82,1	82,5
12:28	81,2	82,3
12:32	80,5	81,3
12:36	80,7	81,1
12:40	81,9	82,3
12:44	81,3	81,1
12:48	81,2	82,4
12:52	81,5	81,8
12:56	82,2	81,4
13:00	82,1	81,6

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 67-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Multímetro Genérico (mA)	Multímetro RadioShack (mA)
13:04	81,3	82,3
13:08	81,4	80,7
13:12	80,9	81,8
13:16	81,6	81,9
13:20	80,6	82,7
13:24	80,4	82,2
13:28	82,9	80,6
13:32	81,1	82,3
13:36	82,5	81,3
13:40	81,9	80,6
13:44	81,9	82,7
13:48	82,1	80,9
13:52	82,1	80,9
13:56	82	82,7
14:00	82,6	81,5

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 68-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Multímetro Genérico (mA)	Multímetro RadioShack (mA)
14:04	80,8	81,4
14:08	81,3	82,6
14:12	82,7	80,8
14:16	80,8	82,2
14:20	81,9	82,3
14:24	82,4	82,8
14:28	82,9	82,7
14:32	81,8	81,5
14:36	81,1	80,7
14:40	82,8	82,7
14:44	80,8	81,3
14:48	80,5	83
14:52	82,3	80,4
14:56	80,5	80,7
15:00	80,6	83
15:04	81,5	80,7
15:08	80,7	82,7
15:12	81,5	82,3
15:16	81,8	81,3
15:20	82,5	83,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 69-3, Tabla 70-3 y Tabla 71-3 se detallan los valores de corriente, algoritmo RSA.

Tabla 69-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
16:04	83	82
16:08	82,3	81,5
16:12	80,5	81,3
16:16	81,8	81,5
16:20	82,4	80,5
16:24	82,4	80,9
16:28	80,7	81,2
16:32	81	80,4
16:36	82,3	83
16:40	81,2	80,4
16:44	82,4	80,7
16:48	82,6	82,5
16:52	81,8	80,9
16:56	82,4	81,9
17:00	80,9	81

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 70-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	Multímetro Genérico (mA)	Multímetro RadioShack (mA)
17:04	81,5	81,2
17:08	80,8	82,6
17:12	81,2	81,4
17:16	82,9	80,7
17:20	81,6	82,3
17:24	81,7	82,5
17:28	81	82
17:32	81,9	82,4
17:36	80,7	80,8
17:40	81,1	82,3
17:44	82,6	81,3
17:48	82,8	81,3
17:52	80,7	82,3
17:56	80,9	80,5
18:00	81,7	81,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 71-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
18:04	82,9	80,5
18:08	81,4	81,9
18:12	82,2	82,4
18:16	82,5	82,6
18:20	82,7	82,7
18:24	82,7	81,4
18:28	80,5	81,2
18:32	81,6	82,4
18:36	82,3	80,5
18:40	81,3	81,7
18:44	82,6	82,8
18:48	81,7	82,5
18:52	81	83
18:56	83	80,9
19:00	83	80,9
19:04	82,5	81,6
19:08	80,7	81
19:12	80,9	80,4
19:16	81,1	80,5
19:20	81,1	81,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 72-3, Tabla 73-3 y Tabla 74-3 se detallan los valores de corriente, algoritmo RSA.

Tabla 72-3. Primer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
20:04	81,7	80,8
20:08	82,8	80,6
20:12	82,7	80,7
20:16	81,3	82,4
20:20	83	81,4
20:24	81,8	82,2
20:28	80,4	82,2
20:32	82,9	80,6
20:36	81,6	82,1
20:40	81	82,9
20:44	82,2	82,4
20:48	82,5	81,5
20:52	81,9	82,1
20:56	81	82,4
21:00	82,3	80,8

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 73-3. Segundo Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
21:04	81,1	82,3
21:08	81,3	81,6
21:12	81,4	81,9
21:16	81,3	81,5
21:20	82,5	81,1
21:24	82,7	80,5
21:28	82,8	80,9
21:32	82,8	80,9
21:36	81	82,1
21:40	81,3	81,9
21:44	82,6	82,1
21:48	83	82,2
21:52	81,1	80,5
21:56	80,5	80,6
22:00	81,1	82,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 74-3. Tercer Periodo de Mediciones (RSA)

RSA (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
22:04	82,8	82,6
22:08	80,8	80,4
22:12	82,6	81
22:16	81,9	82,7
22:20	82,9	80,7
22:24	82,4	81,7
22:28	82,2	81,8
22:32	82	80,7
22:36	81,5	82,9
22:40	82,3	82,1
22:44	83	81,1
22:48	81,9	81
22:52	82,4	80,6
22:56	82,3	80,9
23:00	81,3	81,7
23:04	81,8	82,1
23:08	81	81
23:12	80,6	81,7
23:16	80,6	81,7
23:20	82,6	80,7

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3.1.2 Prueba de Medición a 100 metros con el algoritmo AES 256

En la Tabla 75-3, Tabla 76-3 y Tabla 77-3 se detallan los valores de corriente, realizadas con el algoritmo AES 256, el máximo tamaño de transmisión es de 61 bytes.

Tabla 75-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
8:04	80,8	78,3
8:08	77,4	82,3
8:12	80,9	80,5
8:16	79,3	80,6
8:20	79,1	79,5
8:24	80	82
8:28	81,6	81
8:32	77,7	79,8
8:36	79,9	80,3
8:40	79,3	77,7
8:44	79	80,8
8:48	81,9	78,5
8:52	80,9	81,1
8:56	77,9	81,6
9:00	80,7	78,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 76-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
9:04	80,9	79,1
9:08	81,8	81,6
9:12	77,3	78,2
9:16	81,1	78,2
9:20	81,3	81,8
9:24	78	80,4
9:28	79,5	82,2
9:32	82,3	81,1
9:36	80,4	77,7
9:40	80	80
9:44	80,7	77,6
9:48	80,6	81,9
9:52	79,1	80,4
9:56	79,5	79,2
10:00	78,8	77,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 77-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
10:04	79,3	79,5
10:08	81	80
10:12	78,9	77,9
10:16	77,8	79
10:20	77,5	79,5
10:24	81,1	81,6
10:28	82,3	79,4
10:32	82,2	80,1
10:36	80,5	80,4
10:40	81,6	78,7
10:44	80	79,7
10:48	80,9	78,1
10:52	80,8	79,2
10:56	80,5	82,1
11:00	77,4	78,5
11:04	80,2	80,8
11:08	77,6	80,5
11:12	78,3	80,4
11:16	77,7	81,6
11:20	78,8	79,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 78-3, Tabla 79-3 y Tabla 80-3 se detallan los valores de corriente, AES 256.

Tabla 78-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
12:04	77,8	81,7
12:08	79	81,2
12:12	78,5	80,4
12:16	80,7	81,7
12:20	78,7	79,7
12:24	80	79,9
12:28	78,1	78,3
12:32	80,5	79,4
12:36	80,5	77,9
12:40	77,8	80,7
12:44	80,4	77,6
12:48	80,8	82
12:52	78	79,6
12:56	77,5	78,1
13:00	77,8	78,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 79-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
13:04	80,1	80,4
13:08	79,8	78
13:12	79	79,9
13:16	79,6	81,8
13:20	80,9	81,8
13:24	81,9	81,6
13:28	81,9	79,5
13:32	77,8	79,1
13:36	80,9	78,4
13:40	78	79,2
13:44	81,6	79,3
13:48	80,8	78,9
13:52	81,7	80,8
13:56	77,4	77,4
14:00	79,1	78,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 80-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
14:04	79,4	80,2
14:08	79,5	81,5
14:12	80,1	81,8
14:16	79,7	82
14:20	79,7	77,2
14:24	80,9	78,5
14:28	80,3	79,8
14:32	79,9	78
14:36	81,5	79,7
14:40	79,7	79,7
14:44	78,1	78,7
14:48	79,1	82,4
14:52	80,6	81,8
14:56	77,4	77,3
15:00	79,6	80,5
15:04	80,2	81,5
15:08	82,3	79,3
15:12	79,1	78,6
15:16	81,8	79,6
15:20	81,7	78,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 81-3, Tabla 82-3 y Tabla 83-3 se detallan los valores de corriente, AES 256.

Tabla 81-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
16:04	79,3	81,3
16:08	81,4	80
16:12	80,7	77,8
16:16	79,4	78,7
16:20	79	78,3
16:24	78,6	78,1
16:28	77,2	81,5
16:32	78,2	78,9
16:36	79,7	78,1
16:40	78,2	79,9
16:44	77,7	81,3
16:48	79,3	81,3
16:52	80,1	79,3
16:56	77,8	77,8
17:00	77,5	78,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 82-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
17:04	80,7	79,6
17:08	80,5	81,9
17:12	81,8	80,8
17:16	77,8	81,7
17:20	78,5	79,9
17:24	78,7	82,2
17:28	80,3	81,1
17:32	81,8	78,8
17:36	79,7	77,3
17:40	80	81,1
17:44	79	77,9
17:48	79,7	78,3
17:52	80	81,1
17:56	81	78,4
18:00	79,5	81,6

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 83-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
18:04	81,1	81,6
18:08	78,5	78,9
18:12	79	77,3
18:16	77,7	81
18:20	79,4	80,2
18:24	77,4	78,7
18:28	80,3	78,5
18:32	77,6	78,6
18:36	77,8	82
18:40	79,5	77,9
18:44	79,8	78,7
18:48	79,8	79,8
18:52	81,5	80,6
18:56	80,9	77,3
19:00	81,5	81,4
19:04	78,3	79,1
19:08	78	80,1
19:12	77,2	81,9
19:16	80,3	81,5
19:20	81,2	80,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 84-3, Tabla 85-3 y Tabla 86-3 se detallan los valores de corriente, AES 256.

Tabla 84-3. Primer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
20:04	82	81,8
20:08	79,6	80,8
20:12	78,8	81
20:16	80,5	78,2
20:20	77,2	80,3
20:24	78	81,5
20:28	77,9	81,7
20:32	82,4	79,6
20:36	82,3	81,7
20:40	78,2	82
20:44	80,1	80,8
20:48	78,2	80,3
20:52	81,5	82,3
20:56	78,8	81,1
21:00	80,2	82

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 85-3. Segundo Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
21:04	81,7	80,6
21:08	82,3	78,5
21:12	79,2	82
21:16	79,9	80
21:20	79,3	77,4
21:24	77,7	82
21:28	79,5	77,7
21:32	77,4	80,8
21:36	79,2	77,5
21:40	80	79,8
21:44	79,6	81,6
21:48	77,3	80,8
21:52	80,5	81,7
21:56	82,2	78,9
22:00	77,9	80

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 86-3. Tercer Periodo de Mediciones (AES 256)

AES 256 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
22:04	77,4	82,2
22:08	81,3	78,4
22:12	81,9	78,4
22:16	78,7	78,1
22:20	77,8	78
22:24	81,4	80,4
22:28	78,6	77,7
22:32	79,6	80,5
22:36	79,2	79,1
22:40	77,3	78,9
22:44	81,1	77,3
22:48	77,2	78,5
22:52	80,4	80,3
22:56	77,8	78,6
23:00	77,4	78,7
23:04	77,7	80,4
23:08	79,3	77,9
23:12	78	78,8
23:16	78,7	78,4
23:20	80,1	79,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3.1.3 Prueba de Medición a 100 metros con el algoritmo AES 192

En la Tabla 87-3, Tabla 88-3 y Tabla 89-3 se detallan los valores de corriente, realizadas con el algoritmo AES 192, el máximo tamaño de transmisión es de 61 bytes.

Tabla 87-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
8:04	77,8	79,6
8:08	80,7	79,2
8:12	78,2	80,2
8:16	80,2	81,5
8:20	78,9	80,3
8:24	80,7	80
8:28	80,2	78,7
8:32	79,3	80,7
8:36	81	80,6
8:40	78,4	78,5
8:44	79,6	77,9
8:48	80,6	78,5
8:52	81	79,8
8:56	79,6	78,3
9:00	78,5	78,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 88-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
9:04	78,4	79,6
9:08	78,5	81,2
9:12	81,3	81,1
9:16	78,9	79,2
9:20	77,9	79,2
9:24	77,8	81,5
9:28	79	79,6
9:32	78	80
9:36	79,7	79,8
9:40	79,9	80,9
9:44	78,4	81,5
9:48	79,6	79,4
9:52	79,7	78,4
9:56	77,7	81,1
10:00	79,8	79,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 89-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
10:04	78,5	80,3
10:08	80,5	77,9
10:12	79,1	80,4
10:16	79,5	80,1
10:20	79,9	81,5
10:24	78,6	79,4
10:28	78,6	77,9
10:32	79,5	80,4
10:36	80,8	78,6
10:40	79,8	81,4
10:44	80,9	79,1
10:48	78,7	78,7
10:52	77,9	78,1
10:56	80,5	79,3
11:00	80,3	78,7
11:04	78,7	78,3
11:08	80,8	78,5
11:12	78	78,9
11:16	79,1	78,4
11:20	80,3	78,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 90-3, Tabla 91-3 y Tabla 92-3 se detallan los valores de corriente, AES 192.

Tabla 90-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
12:04	80,5	81,2
12:08	81	80,9
12:12	80,4	77,9
12:16	79,8	78,3
12:20	78,6	78,2
12:24	79,1	81,1
12:28	78,1	78,9
12:32	78,5	80
12:36	81,5	79,2
12:40	81,3	78
12:44	81,1	79
12:48	78,1	79,6
12:52	80,3	80,3
12:56	78,7	79,9
13:00	79,5	81,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 91-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
13:04	81,5	81,1
13:08	81	81
13:12	80,1	79,6
13:16	77,9	77,9
13:20	81	79,9
13:24	80,6	78,4
13:28	80,5	79,7
13:32	78,4	80,2
13:36	80,6	79,6
13:40	81,3	78,6
13:44	79,7	80,3
13:48	81,1	78,8
13:52	79,8	79
13:56	80,6	77,7
14:00	80,4	79,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 92-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
14:04	80,2	81,1
14:08	79,9	79
14:12	81,2	78,1
14:16	79,5	80,2
14:20	80,9	78,4
14:24	78,8	78
14:28	78,5	81,4
14:32	78,9	80,9
14:36	79,4	81,2
14:40	81,3	79,2
14:44	78,2	80,5
14:48	79,8	77,8
14:52	81,2	79,8
14:56	79	81,4
15:00	80,3	78,2
15:04	79	78,2
15:08	78,1	80,1
15:12	81,5	80
15:16	81,3	79,7
15:20	80,5	79,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 93-3, Tabla 94-3 y Tabla 95-3 se detallan los valores de corriente, AES 192.

Tabla 93-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
16:04	79,8	79,9
16:08	79	77,8
16:12	81,4	81,2
16:16	77,8	80,3
16:20	77,8	79,9
16:24	79,6	78,9
16:28	79,5	78,1
16:32	79,3	80,9
16:36	79,7	79,5
16:40	78,3	80,9
16:44	78,1	79
16:48	81	80,9
16:52	79,3	79,6
16:56	80,7	81,4
17:00	78,6	78,5

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 94-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
17:04	77,7	78
17:08	79,4	80,3
17:12	80,1	81
17:16	81	77,7
17:20	81,2	80,9
17:24	78,2	78,8
17:28	81,1	77,8
17:32	78,5	78,5
17:36	79,1	81,2
17:40	80,6	79,5
17:44	80,2	80,3
17:48	77,9	81,5
17:52	77,8	80,9
17:56	78,1	79,1
18:00	78,5	81,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 95-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
18:04	81,2	80,7
18:08	79,1	79,3
18:12	78,1	80,4
18:16	78	79,6
18:20	79	79,4
18:24	78,3	78,8
18:28	78	78,9
18:32	80,7	79,7
18:36	78,7	78,8
18:40	81,4	79,5
18:44	80,3	77,9
18:48	79	81
18:52	80,8	77,7
18:56	80,5	81
19:00	79,4	80,2
19:04	78,9	81,3
19:08	80,8	80,4
19:12	81,3	81,4
19:16	78,6	79,6
19:20	80,9	81,4

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 96-3, Tabla 97-3 y Tabla 98-3 se detallan los valores de corriente, AES 192.

Tabla 96-3. Primer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
20:04	81,4	79
20:08	78,2	78,9
20:12	81,2	78,4
20:16	77,7	78,5
20:20	81,3	80,6
20:24	79,1	78
20:28	79,2	79,4
20:32	78,6	78,8
20:36	80,7	81,2
20:40	79	79,9
20:44	78,9	80,1
20:48	78,5	79,6
20:52	79,8	81,2
20:56	77,9	81,4
21:00	80,1	80

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 97-3. Segundo Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
21:04	78,4	78,1
21:08	77,9	81,5
21:12	81,3	81,3
21:16	79,5	81,3
21:20	78,1	79,7
21:24	78,6	80,8
21:28	78	80,5
21:32	79,9	80,5
21:36	80,2	78,5
21:40	79,7	79,2
21:44	81,4	80,2
21:48	79,3	78,6
21:52	79,4	81,2
21:56	78,6	79,8
22:00	81	80,6

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 98-3. Tercer Periodo de Mediciones (AES 192)

AES 192 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
22:04	78,6	78,9
22:08	80,7	79,2
22:12	77,8	78,1
22:16	79,5	79,1
22:20	80,8	81,4
22:24	80,2	77,8
22:28	79,3	79
22:32	79,7	79,7
22:36	80,8	80,8
22:40	78,8	79,2
22:44	79,7	80,3
22:48	77,9	78
22:52	80,9	78,2
22:56	79,2	79,2
23:00	79,2	79,2
23:04	78,4	78,6
23:08	80,4	79,3
23:12	78	79,5
23:16	78,3	81,1
23:20	78,1	79,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3.1.4 Prueba de Medición a 100 metros con el algoritmo AES 128

En la Tabla 99-3, Tabla 100-3 y Tabla 101-3 se detallan los valores de corriente, realizadas con el algoritmo AES 128, el máximo tamaño de transmisión es de 61 bytes.

Tabla 99-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
8:04	75,6	79,3
8:08	80	78,2
8:12	78,6	80,1
8:16	79,7	76
8:20	76,3	79,7
8:24	78,8	75,7
8:28	75,6	76,9
8:32	77,7	79,8
8:36	76,1	75,9
8:40	77,7	76,9
8:44	78	76,5
8:48	77,1	79,9
8:52	78,1	78,2
8:56	77,1	75,6
9:00	78,1	77,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 100-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
9:04	78,9	78,9
9:08	77	77,3
9:12	79,6	78
9:16	78,9	79,4
9:20	79,4	77,8
9:24	76,1	77,3
9:28	75,9	79,8
9:32	79,5	75,4
9:36	77,3	78,4
9:40	79,8	79,1
9:44	78	79,2
9:48	75,5	78,8
9:52	78,4	78
9:56	76,8	76,4
10:00	79,8	78,5

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 101-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
10:04	76,5	78,8
10:08	80,1	77,5
10:12	75,4	78
10:16	77,7	75,6
10:20	79,4	77
10:24	77,9	76,3
10:28	79,8	79,6
10:32	79,5	79,9
10:36	77,2	78,9
10:40	78,5	78
10:44	78,2	76,8
10:48	77,7	79,6
10:52	79,9	76,9
10:56	78,8	79,1
11:00	75,8	78,4
11:04	79	75,6
11:08	78,1	76,3
11:12	75,6	79,2
11:16	78,1	76,5
11:20	79,5	77,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 102-3, Tabla 103-3 y Tabla 104-3 se detallan los valores de corriente, AES 128.

Tabla 102-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
12:04	79,5	76,3
12:08	75,5	77,5
12:12	77,1	76,4
12:16	75,5	78
12:20	78,1	77,4
12:24	77,3	78
12:28	79,4	78,6
12:32	77,9	78,2
12:36	78,3	78,4
12:40	78,4	79,5
12:44	78,3	78,5
12:48	78,3	77,3
12:52	77,5	79,1
12:56	77,9	80,1
13:00	79,3	79,5

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 103-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
13:04	78,1	76,2
13:08	75,5	79
13:12	79	77,7
13:16	76,3	77,4
13:20	79,9	79,7
13:24	78,2	78,3
13:28	78,6	75,6
13:32	76,8	78,5
13:36	75,7	76,6
13:40	77,9	78,1
13:44	77,1	78,6
13:48	77,2	77,3
13:52	77,6	79,8
13:56	78	77,2
14:00	76,1	77

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 104-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
14:04	76,6	76,3
14:08	78,4	76,4
14:12	80,1	76,8
14:16	79,5	77,6
14:20	79,2	75,5
14:24	76,9	80
14:28	77,1	78,9
14:32	76,8	77,7
14:36	78	77,3
14:40	76,8	77,2
14:44	76,9	79,2
14:48	75,9	75,4
14:52	76,4	76
14:56	75,7	75,7
15:00	78,7	79,8
15:04	76,7	77,7
15:08	77,7	78,5
15:12	75,5	75,8
15:16	80	78
15:20	77,9	75,7

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 105-3, Tabla 106-3 y Tabla 107-3 se detallan los valores de corriente, AES 128.

Tabla 105-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
16:04	79,2	79,7
16:08	78,7	77,3
16:12	78,2	79,3
16:16	78,2	75,6
16:20	77,3	75,8
16:24	75,7	77,9
16:28	76,2	79,5
16:32	78,6	79,5
16:36	78,3	78
16:40	76,3	79,4
16:44	79,3	79,2
16:48	78,3	79,4
16:52	77,6	79,5
16:56	79,9	79,8
17:00	76,8	79,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 106-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
17:04	79,8	76,4
17:08	78,9	76,5
17:12	80	75,6
17:16	78,4	79,5
17:20	78,8	77,4
17:24	77,3	78,2
17:28	80	77,8
17:32	75,7	76,5
17:36	79,9	79,8
17:40	79,9	78,1
17:44	79,7	79,8
17:48	79	79,1
17:52	79,8	78,2
17:56	77,5	76,3
18:00	78,7	75,6

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 107-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
18:04	77,2	76,6
18:08	75,7	79,3
18:12	79,5	78,4
18:16	77,2	79,9
18:20	76,4	75,6
18:24	76,7	80
18:28	80	77,4
18:32	76,1	77,4
18:36	77,4	75,9
18:40	79,7	77,1
18:44	78,7	79,7
18:48	79,8	76,5
18:52	75,8	78,9
18:56	75,8	75,5
19:00	76,7	77,9
19:04	78,4	79,7
19:08	76	77,4
19:12	77,9	79,9
19:16	76,3	80,1
19:20	77	79,5

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 108-3, Tabla 109-3 y Tabla 110-3 se detallan los valores de corriente, AES 128.

Tabla 108-3. Primer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
20:04	78,5	78,5
20:08	78,2	76,4
20:12	77,6	77,5
20:16	78,8	77,1
20:20	78,7	77,5
20:24	76,3	77,4
20:28	76,9	75,9
20:32	77	76,5
20:36	79,7	77,2
20:40	76,1	75,7
20:44	75,7	78,7
20:48	75,4	75,8
20:52	80,1	77,5
20:56	78,7	79,3
21:00	78,4	75,7

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 109-3. Segundo Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
21:04	79,3	76,8
21:08	79,4	78,9
21:12	80	79,6
21:16	76,6	75,9
21:20	76,1	76,5
21:24	78,9	76,7
21:28	78,7	77,6
21:32	78,5	77,1
21:36	79,6	78,5
21:40	76,3	79,7
21:44	76,1	78,1
21:48	78,8	75,5
21:52	77,2	77
21:56	76,4	78
22:00	78,2	79,1

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 110-3. Tercer Periodo de Mediciones (AES 128)

AES 128 (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
22:04	78,4	79
22:08	77,5	79,2
22:12	79,1	75,5
22:16	77,3	79,9
22:20	76,9	79,3
22:24	78,6	78,4
22:28	79,2	76
22:32	78,1	76,2
22:36	76,9	77,5
22:40	77,8	75,6
22:44	75,8	77,7
22:48	79,6	79,4
22:52	76,6	76,4
22:56	78,6	76,7
23:00	79,7	75,6
23:04	76,4	77,8
23:08	76,8	78,7
23:12	77,9	76,6
23:16	79,7	78,3
23:20	75,9	78,2

Realizado por: Andrés Solís, Ítalo Parreño, 2019

3.3.1.5 Prueba de Medición a 100 metros con Texto Plano

En la Tabla 111-3, Tabla 112-3 y Tabla 113-3 se detallan los valores de corriente, enviados en texto plano, el máximo tamaño de transmisión es de 35 bytes.

Tabla 111-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
8:04	77,6	79,6
8:08	78,4	74,8
8:12	77,6	79,1
8:16	74,8	77,7
8:20	75,4	79,4
8:24	76,4	78,5
8:28	75,8	78,5
8:32	79,1	77,6
8:36	78,1	78,6
8:40	78,2	77,6
8:44	75,7	79,7
8:48	74,8	76,4
8:52	78,4	75,7
8:56	78,7	76,2
9:00	77,4	79,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 112-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
9:04	78	79,5
9:08	78,3	77,9
9:12	75,9	78,8
9:16	74,8	77
9:20	77,7	79,9
9:24	75,7	75,4
9:28	77,1	77,1
9:32	78,5	77
9:36	78,1	79,4
9:40	75,1	76
9:44	76,4	75,6
9:48	77,5	76,8
9:52	76,7	75,6
9:56	76,3	75,4
10:00	76,1	75,9

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 113-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
10:04	79,5	78
10:08	77,9	78,4
10:12	74,7	78,2
10:16	75,6	77,6
10:20	78,5	78,2
10:24	76,5	78,7
10:28	76,6	74,7
10:32	76,8	75,8
10:36	77,2	75,5
10:40	74,9	76,4
10:44	76,5	78,4
10:48	76,1	77,5
10:52	75,3	75,7
10:56	75,3	77
11:00	79,2	79,1
11:04	77,3	78,6
11:08	77,1	78
11:12	77,1	75,3
11:16	78,9	76,1
11:20	75,2	77,8

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 114-3, Tabla 115-3 y Tabla 116-3 se detallan los valores de corriente, texto plano.

Tabla 114-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
12:04	76,4	77,5
12:08	79	74,5
12:12	77,1	75,8
12:16	78,3	78,3
12:20	77,6	75,3
12:24	77	76,3
12:28	76,1	78,8
12:32	78,9	75,8
12:36	76,9	79,1
12:40	77,4	75,5
12:44	77,8	78,4
12:48	77,4	77,7
12:52	78,1	79,5
12:56	78,9	76,3
13:00	79,2	76,3

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 115-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
13:04	78,6	76,4
13:08	75,6	75,3
13:12	74,8	79,5
13:16	78,5	78,8
13:20	75	79,4
13:24	75,9	78,2
13:28	77,7	75,6
13:32	78,2	77,6
13:36	78	77,2
13:40	75,9	77,9
13:44	78,8	77,2
13:48	77,7	75,3
13:52	75,1	76,9
13:56	79,1	76,6
14:00	78,3	77,6

Realizado por: Andrés Solís, Ítalo Parreño, 2019

Tabla 116-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
14:04	74,7	76,1
14:08	77,8	74,6
14:12	77,8	79,6
14:16	76,2	75,5
14:20	78,6	78,9
14:24	75,8	76,9
14:28	78,7	76,8
14:32	78,2	77,7
14:36	78,2	74,8
14:40	75	76,8
14:44	74,9	75,7
14:48	78,1	75,6
14:52	77,9	74,9
14:56	78,9	77,9
15:00	75,9	76,2
15:04	77,9	79,8
15:08	76,8	78,7
15:12	79,6	76,3
15:16	76,6	78,2
15:20	76,5	75,8

Realizado por: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 117-3, Tabla 118-3 y Tabla 119-3 se detallan los valores de corriente, texto plano.

Tabla 117-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
16:04	77	78,2
16:08	75,6	79,6
16:12	78,7	75,7
16:16	78,4	75,8
16:20	76,7	78,5
16:24	75,6	74,6
16:28	78	78,3
16:32	77,3	78,8
16:36	74,7	76,3
16:40	77,5	76,6
16:44	75,9	74,8
16:48	78,7	75,2
16:52	74,8	76,1
16:56	77,1	75
17:00	75,4	76,5

: Andrés Solís, Ítalo Parreño, 2019

Tabla 118-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
17:04	77,3	76,7
17:08	75,3	76,4
17:12	76,5	78,8
17:16	78,8	77
17:20	74,7	78,7
17:24	79,2	78
17:28	76,4	74,7
17:32	77,5	75,1
17:36	76,9	76,9
17:40	77,9	77,2
17:44	75,7	79,2
17:48	76,5	77,8
17:52	77,6	76,6
17:56	78,9	78,9
18:00	74,9	76,6

Fuente: Andrés Solís, Ítalo Parreño, 2019

Tabla 119-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
18:04	79	79,4
18:08	76,2	77,5
18:12	75	79,4
18:16	76,5	78,5
18:20	75,1	79,5
18:24	78,8	78
18:28	75,4	75,9
18:32	75	79,8
18:36	77,4	77,2
18:40	75	78,1
18:44	76,1	77,3
18:48	75,2	78,9
18:52	79,7	79,8
18:56	78,6	78,2
19:00	75,7	78,5
19:04	76,8	78,9
19:08	78,9	74,9
19:12	75,8	74,9
19:16	79,5	76,8
19:20	78	75,5

Fuente: Andrés Solís, Ítalo Parreño, 2019

En la Tabla 120-3, Tabla 121-3 y Tabla 122-3 se detallan los valores de corriente, texto plano.

Tabla 120-3. Primer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
20:04	78	78,5
20:08	78,8	78
20:12	77,3	75,4
20:16	78,6	76,4
20:20	75,1	75
20:24	77,2	76,8
20:28	77,7	76,6
20:32	79,6	74,8
20:36	79,1	78,2
20:40	79,1	77,9
20:44	75,8	78,9
20:48	75,5	76,1
20:52	77,7	79,6
20:56	79,3	78,8
21:00	76,4	76,1

Fuente: Andrés Solís, Ítalo Parreño, 2019

Tabla 121-3. Segundo Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
21:04	76,2	74,9
21:08	75,1	77,2
21:12	79	76,7
21:16	77,5	79,3
21:20	78,7	76,6
21:24	77,3	78,9
21:28	77,2	79,9
21:32	78,8	75
21:36	77,1	79,6
21:40	79,3	76,7
21:44	78,7	79,9
21:48	76,8	78,7
21:52	79,5	79,4
21:56	78	74,8
22:00	79	79,5

Fuente: Andrés Solís, Ítalo Parreño, 2019

Tabla 122-3. Tercer Periodo de Mediciones (Texto Plano)

Texto Plano (100 metros)		
Hora	**Multímetro Genérico (mA)**	**Multímetro RadioShack (mA)**
22:04	76,5	78,3
22:08	78,7	78,8
22:12	78,8	76,8
22:16	76,6	74,6
22:20	77,5	76,9
22:24	76,4	77,4
22:28	75,6	75,4
22:32	79	78,1
22:36	75,5	76,4
22:40	78,7	75,1
22:44	79,3	75,8
22:48	76,6	75,1
22:52	76,4	77,3
22:56	79,4	78,3
23:00	78,7	78,6
23:04	76,3	75,4
23:08	79	78,4
23:12	78,5	74,8
23:16	78,5	77,5
23:20	77,8	76,5

Fuente: Andrés Solís, Ítalo Parreño, 2019

3.3.2 Comparación entre texto plano y los diferentes algoritmos en 100 metros

Tabla 123-3. Datos Promedio De los Algoritmos Realizados en 100 metros

100 metros (100m)					
Medidores	**Algoritmos**				
	Texto Plano	**AES 128**	**AES 192**	**AES 256**	**RSA**
Multímetro Genérico Serie 830	77,2 mA	77,9 mA	79,5 Ma	79,6 mA	81,7 mA
Multímetro RadioShack	77,2 mA	77,8 mA	79,6 mA	79,8 mA	81,6 mA

Fuente: Andrés Solís, Ítalo Parreño, 2019

En el Gráfico 2-3 observamos la comparación entres texto plano y los diferentes algoritmos utilizados en esta investigación utilizando dos dispositivos de medición, un multímetro genérico Serie 830 representado en color azul y un multímetro RadioShack representado con color naranja, a continuación, detallaremos los valores:

- Entre el algoritmo AES 128 y texto plano existe una diferencia entre 0,6 a 0,7 mA.
- Entre el algoritmo AES 192 y texto plano existe una diferencia entre 2,3 a 2,4 mA.
- Entre el algoritmo AES 256 y texto plano existe una diferencia entre 2,4 a 2,6 mA.
- Entre el algoritmo RSA y texto plano existe una diferencia entre 4,4 a 4,5 mA.

En resumen, se puede notar que el algoritmo RSA es el más consumista con un valor de corriente entre 4,4 a 4,5 mA, por el contrario, el algoritmo que menos corriente consume es AES 128 con un valor de entre 0,6 a 0,7 mA.

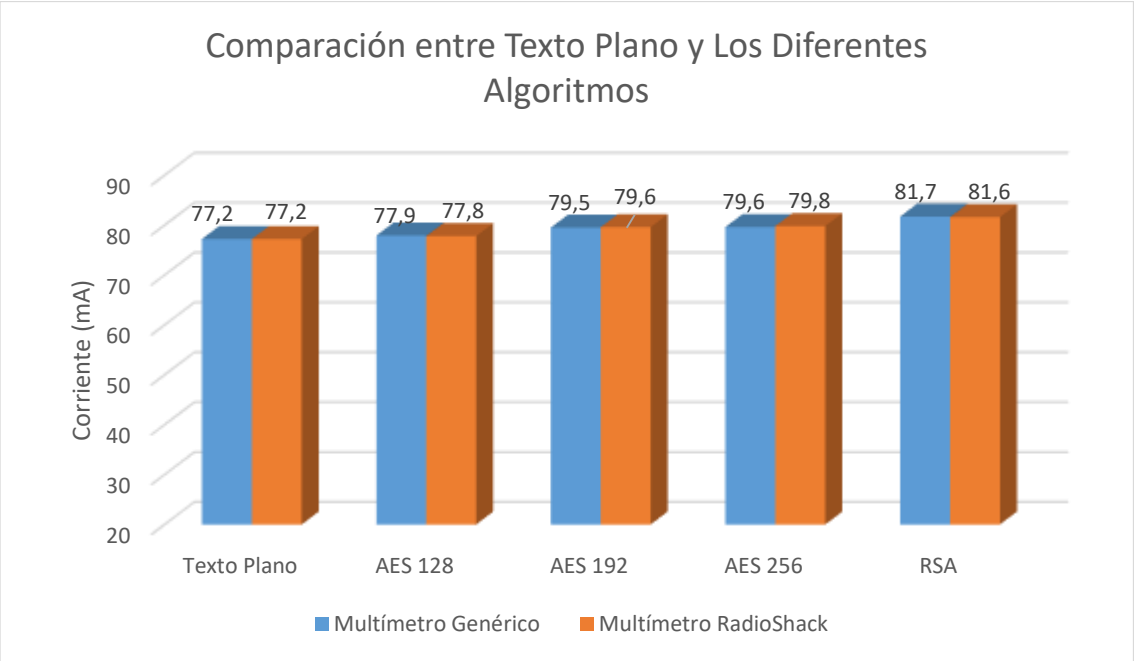

Gráfico 2-3. Comparación de los algoritmos frente a texto plano en 100 metros

Fuente: Andrés Solís, Ítalo Parreño, 2019

3.3.3 Porcentajes de Descarga

Tabla 124-3. Datos Porcentuales de Descarga en una distancia de 100 metros

Número de Sensor	Lectura Inicial	Lectura Final
Texto Plano	100%	100%
AES 128	100%	94%
AES 192	100%	81%
AES 256	100%	80%
RSA	100%	48%

Fuente: Andrés Solís, Ítalo Parreño, 2019

Los datos de la Tabla 124-3 son las medidas que se obtienen de los sensores internos de la tarjeta Waspmote, el cual nos indica el desgaste de la batería por medio de un valor porcentual, acompañado del valor en voltios que la batería tiene en el momento que la tarjeta comienza su funcionamiento. Los comandos que se utilizaron para obtener esta información son:

- PWR.getBatteryLevel
- PWR.getBatteryVolts

En la Figura 5-3 se ilustra cómo se visualizan los datos obtenidos tanto en nivel de carga y el valor en voltaje que la batería posee en el momento que a tarjeta solicita esa información a sus sensores internos.

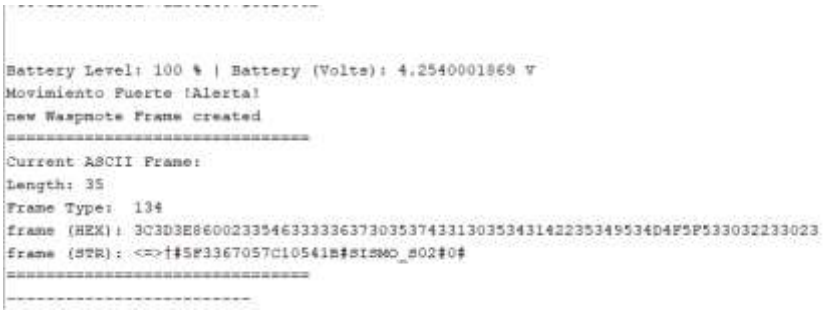

Figura 5-3. Datos obtenidos de la tarjeta

Fuente: Andrés Solís, Ítalo Parreño, 2019

Otra prueba realizada es por la distancia de 100 metros obteniendo valores mostrados en la Tabla 124-3, el periodo de tiempo para el análisis de los datos es de doce horas. Estos datos son:

- En él envió de información enviada en texto Plano, los nodos sensores luego de tres horas y veinte de trabajo y con una carga inicial de 100% se mantiene ese valor al finalizar el tiempo de trabajo para el estudio.
- En él envió de información encriptada por el algoritmo AES 128, los nodos sensores con la carga inicial al 100% al transcurrir las tres horas y veinte minutos de trabajo en las peores condiciones su carga final es de 94% de la capacidad de la batería.
- En él envió de información encriptada por el algoritmo AES 192, los nodos sensores con el nivel de batería inicial al 100%, la medida obtenida al terminar las tres horas y veinte minutos de trabajo es el 81% de la capacidad de la batería.
- En él envió de información encriptada por el algoritmo AES 256, los nodos sensores con su lectura inicial de la capacidad de batería de 100%, la medida que se obtuvo al pasar las tres horas y veinte minutos de trabajo es el 80% de la capacidad de la batería.
- En él envió de información encriptada por el algoritmo RSA, los nodos sensores con un nivel de batería inicial del 100%, al transcurso de tres horas y veinte minutos de trabajo su nuevo nivel de capacidad de batería es el 48%.

CONCLUSIONES

- Al analizar los algoritmos teniendo como punto inicial la propiedad de la información conocida como confidencialidad y apoyándonos en que Waspmote ofrece dos tipos de algoritmos con estas cualidades tanto simétrico en el caso de AES 128, 192 y 256 como asimétrico RSA se precisó tomar ambos algoritmos para la realización de pruebas y determinar cuál ofrecería protección de los datos que enviamos sin comprometer el consumo de la batería y de tal manera prolongar su vida útil evitando perder conectividad de los nodos sensores, el tiempo escogido para la prueba fue de cuatro minutos que corresponde al periodo que históricamente duro el sismo más fuerte ocurrido desde entonces con una intensidad de 9,5 en la escala de Richter.
- Se realizaron pruebas de las dos topologías siendo estas malla y estrella, comparándolas entre sí, dando como resultado que la topología estrella en su implementación tiene un menor consumo de energía y, por lo tanto, es la mejor opción ya que tiene un bajo empleo en cuestión de recursos energéticos y cumple con los requisitos de este estudio.
- Se implementó el prototipo de una red WSN basado en la topología estrella a utilizar con 5 sectores, llamados así ya que uno de estos sectores representa un nodo de la red. Al tener que monitorear ondas sísmicas el prototipo necesitaba generar movimientos para que esa información sea detectada y envía por la tarjeta, para ello se utilizó una centrina controlada por un circuito PWM para tener niveles de movimiento. De esta manera simulamos un movimiento, el cual registrado en la historia ha sido el peor caso, con esto tomamos valores lo más reales posibles que permitieron que se evalué la eficiencia energética.
- Al realizar la comunicación extrema a extremo “Canal No Seguro”, la cual enviaba toda la información en texto plano, teniendo así brechas en la seguridad de nuestra información sensible. Es así que para la comunicación extremo a extremo “Canal Seguro” en la tarjeta se implementó los algoritmos de encriptación asimétrico y simétrico. La tarjeta de forma nativa posee algoritmos como AES de 128, 192 y 256 y RSA, permitiendo así que la información que los nodos envíen sea encriptada y si en un momento de la comunicación es interceptada su descifrado sea complicado debido a que el atacante no conoce en que algoritmo de encriptación se está enviando esa información. De esta manera aseguramos que la información sensible que se está enviando llegue de forma segura a su destino evitando que se generen falsas alarmas.

- Para verificar como se ve afectada la eficiencia energética de cada tarjeta Nodo Sensor al implementar los algoritmos de encriptación para tener una comunicación extrema a extremo “Canal Seguro”, se la realizo con dos diferentes dispositivos que nos permitieron conocer el desgaste que se produce al momento de enviar la información, siendo estos dispositivos: multímetro Genérico y un multímetro RadioShack. Luego de obtener los 200 datos en texto plano y en los algoritmos de encriptación: AES 128, 192,256 y RSA; trabajando en las peores condiciones es decir enviando el mensaje durante 13 horas con 20 minutos cada uno de ellos. Obteniendo los siguientes porcentajes de descarga: AES 128: 7%; AES 192: 19%; AES 256: 20% y RSA: 52%. Con estos resultados presentados se concluye que el algoritmo que nos permite tener un canal seguro de comunicación y a su vez una eficiencia energética óptima es AES de 128.

RECOMENDACIONES

- Para una mejor utilización de las tarjetas Waspmote de la marca Libelium se recomienda familiarizarse con el manual que proporciona la página de la marca donde además de la guía también se puede encontrar la interfaz en la cual se realizara la programación y donde se observaran los resultados, a su vez se encuentran ejemplos de programas con los comandos básicos para una mejor comprensión de cómo funciona la plataforma.
- Se recomienda que para el reconocimiento entre la PC y las tarjetas Waspmote mediante el cable serial conectado por la terminal usb, se instale los controladores FTDI que el mismo solicita al momento de la conexión, caso contrario no existirá comunicación entre la tarjeta y la plataforma de programación impidiendo trabajar con la tarjeta.
- Es imperativo poseer la batería de la tarjeta Waspmote, conectarla al dispositivo y dejarla conectada para empezar su carga, ya que, si se pretende utilizar la tarjeta sin tener conectada y cargada la batería, el dispositivo no funcionara de ningún modo sea que el programa se cargue mediante el cable serial de manera satisfactoria, además para que el programa insertado en la tarjeta empiece a correr se debe cambiar de posición a los selectores de la tarjeta desde ON a OFF, como también el selector de WatchDog y el selector de hibernación.
- Es necesario tener los firmwares de XCTU actualizado para poder configurar los Xbee, ya que, si no tienen actualizado estos, toda la información que queríamos escribir en os Xbee no será reconocida y se perderá tiempo al intentar encontrar el error. Por otro si las configuraciones escritas sobre un Xbee las desea borrar para volver a escribir, recomendable que regrese a las configuraciones por default para luego escribir las nuevas de esta forma garantiza que la información nueva será receptada por el Xbee.
- Para mantener un equilibrio entre Seguridad y Eficiencia Energética al finalizar las diferentes pruebas realizadas recomendamos utilizar en una Red WSN en la topología en estrella se utilice el algoritmo AES DE 128.
- En cuanto a trabajos futuros con respecto al tema desarrollado se recomienda que pueden medir otros parámetros como: Latencia, Throughput; de esta forma se podría mejorar el estudio realizado y verificar si al medir estos nuevos parámetros el algoritmo que el estudio presente arrogo sigue siendo el más óptimo.

BIBLIOGRAFIA

1. **Akyildiz Ian F. , Melodia Tommaso, Chowdhury Kaushik R..** *Asurvey on wireless multimedia sensor networks* s.l. : ScienceDirect, 2006, pág. 35. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1389128606002751

2. **Arano Carlos García.** Impacto de la Seguridad en Redes Inalámbricas de Sensores IEEE 802.15.4.[En línea] (Tesis) (Maestría) *Universidad Complutense Madrid.* 2010. [Citado el: 10 de Mayo de 2018.] Pag. 4-5-6. Disponible en : https://eprints.ucm.es/11312/1/Memoria_Fin_de_Master__Carlos_Garc%C3%ADa_Arano.pdf.

3. **Arduino.** Arduino. [En línea] [Citado el: 21 de Mayo de 2018.] Disponible en: https://www.arduino.cc/en/Guide/Introduction#.

4. **Díaz Suárez Alvaro.** Sistemas Embebidos en Red Seguros. *Departamento de Tecnología Electrónica e Ingeniería de Sistemas y Automática.* [En línea] (Tesis) (Doctorado) *Universidad de Cantabria.* 27 de 06 de 2017. [Citado el: 18 de Mayo de 2018.] Pag. 16. Disponible en : https://www.tesisenred.net/handle/10803/404815

5. **Lopes Pereira R. , Trindade J. ,Goncalves F. , Barbosa D. , Vazao T.** *A wireless sensor network for monitoring volcano-seismic signals* s.l. : Nat. Hazards Earth Syst. DiscussPortugal, 2014, pág. 3126. Disponible en : www.nat-hazards-earth-syst-sci.net/14/3123/2014/

6. **Garbarino Jimena.** Protocolos para redes inalámbricas de sensores. [En línea] (Tesis) (Ingeniería) *Universidad de Buenos Aires.* 2011. [Citado el: 24 de Junio de 2018.] Pag. 40. Disponible en: http://materias.fi.uba.ar.

7. **Ibrahim H. , Ilianca A. , Perron J.** *Energy storage systems-Characteristics and comparisons* s.l. : SciencieDirect, 2007, págs. 1238-1239. Disponible en: www.elsevier.com/locate/rser

8. **Jáuregui Milone José Luis s.** Localización de un Sismo utilizando una Estación de Tres Componentes.[En línea] (Tesis) (Licenciatura) *Universidad Mayor de San Marcos.* 2005. [Citado el: 12 de Julio de 2018.] Pag. 10-11. Disponible en : http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/millones_jj/millones_jl.pdf.

9. **Libelium Comunicaciones Dsitribuidas SL.** Cookin Hacks. *Waspmote - Wireless Sensor Networks Open Source Platform.* [En línea] [Citado el: 23 de Mayo de 2018.] Disponible en: https://www.cooking-hacks.com/documentation/tutorials/waspmote/.

10. **Maraiya, Kiran, Kant, Kamal y Gupta, Nitin.** *Architectural Based Data Aggregation* Noida : Department of Computer Science and Engineering, 2015, Department of Computer Science and Engineering, págs. 2,3. Disponible en: https://pdfs.semanticscholar.org/ba66/af102bf63566980e4f4e598272c2ca86a6c8.pdf&ved=2ahUKEwil_4vXjaDhAhWMt1kKHfmKC0gQFjAAegQIARAB&usg=AOvVaw190eS3V6J8N3PNZJMBTVRN

11. **Matin M.A. y Islam M.M.** *Overview of Wireless Sensor Network.* Dhaka : s.n. 2012 [En línea].Disponible en: https://www.researchgate.net/publication/272832872_Overview_of_Wireless_Sensor_Network

12. **Moreno Rocabado Sergio Hernán.** Caso de estudio de Comunicaciones Seguras sobre Redes Móviles AD HOC. [En línea] (Tesis) (Maestría) *Universidad Nacional de la Plata.*12 de 2013. [Citado el: 11 de Noviembre de 2018.] Pag. 87. Disponible en: http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Rocabado_Moreno_Sergio.pdf.

13. **Moya Guaña, Edison Javier.** Diseño de una Red de Sensores Inalámbricos (WSN) para monitorear parámetros relacionados con la agricultura. [En línea] (Tesis) (Ingeniería) *Repositorio Digital EPN*. 09 de 10 de 2016. [Citado el: 15 de Abril de 2018.] Pag. 13. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/16809.

14. **Msi.** *Tech manual-Piezo Film Sensors.* 2008. págs. 3-4. Disponible en: https://www.sparkfun.com/datasheets/Sensors/Flex/MSI-techman.pdf&ved=2ahUKEwjjhsWWh6DhAhUEuVkKHWUdDokQFjAAegQIAhAB&usg=AOvVaw0_WuDDbwxDJIa22U_Vsv4v

15. **OpenSource.** OpenSource. *What is a Raspberry?* [En línea] [Citado el: 15 de Mayo de 2018.]. Disponible en: https://opensource.com/resources/raspberry-pi.

16. **Parallax.** Piezo-Film-Documentation. [En línea] [Citado el: 20 de 06 de 2018.] Pag. 1. Disponible en: www.parallax.com.

17. **Rawat, Priyanka, y otros.** *Wireless Sensor Networks: recent developments* Lille : The Journal of Supercomputing, 2013. Disponible en: https://portail.telecom-bretagne.eu/publi/public/fic_download.jsp?id=30791

18. **Sempere, Joaquín Alavés.** Monitorización remota de las condiciones ambientales de un entorno delimitado. [En línea] (Tesis) (Ingeniería) *Escuela Politécnica Superior*. 06 de 2015. [Citado el: 2 de Mayo de 2018.] Pag. 23-24. Disponible en : https://rua.ua.es/dspace/bitstream/10045/47513/1/Monitorizacion_remota_de_las_condiciones_ambientales_ALAVES_SEMPERE_JOAQUIN.pdf.

19. **Stallings, William.** *Cryptography and Network Security: Principles and Practices.* Prentice Hall, 2005. págs. 28-29-30.

20. **Vargas A. Juan, García Lilia, Martinez Sylvia, Chávez Laura, Muñoz Diego.** *Cifrado de datos con algoritmo AES usando programación multihilo en Java*. 2010, pág. 3.Disponible en: http://www.itvictoria.edu.mx/personal/art_investigacion/AES_paralelo_2010.pdf&ved=2ahUKEwjR1c2_i6DhAhXJwFkKHaFYD1wQFjAAegQIBBAB&usg=AOvVaw1oUa18Y1JPjwWQmg2QqNF6

21. **Wegner, Philip.** Secure Edge Networks. *4 Big Issues with Outdoor Wireless Networking.* [En línea] 26 de Septiembre de 2011. [Citado el: 10 de Abril de 2018.] Disponible en: https://www.securedgenetworks.com/blog/4-Big-Issues-with-Outdoor-Wireless-Networking.

ANEXOS

Anexo A: Programa diseñado para las tarjetas *Waspmote*

```
// Put your libraries here (#include ...)
#include "WaspAES.h"
#include <WaspRSA.h>
#include "WaspXBee802.h"
#include "WaspFrame.h"

float val;
int c = 0;
int f = 0;

// Destination MAC address
////////////////////////////////////////
char RX_ADDRESS[] = "0013A20040D7CE50";
////////////////////////////////////////

//char modulus[] =
//"7ebd3e97454cc46ebcf758a5b0b1ddfc" \
//"4775878048968cf3b2aaa0e34b8b0553" \
//"7c871203caa31d77aa0616571ecf388b" ;

// define exponent for public key 'e'
// This key is defined as HEX format:
// 0x00010001 = 65537 which is a prime number
//char public_exponent[] = "10001";

//char message[] = "5369736d6f20533031";
//char message[] = "5369736d6f20533032";
//char message[] = "5369736d6f20533033";
//char message[] = "5369736d6f20533034";
//char message[] = "5369736d6f20533035";

// 3. variable to store the encrypted message
char enc_message[300];
```

```
// Define the Waspmote ID
char mote_ID[] = "NODO_02";

// define variable
uint8_t error;
// Define a 16-Byte (AES-128) private key to encrypt message
//char password[] = "libeliumlibelium";

// Define a 24-Byte (AES-192) private key to encrypt message
char password[] = "libeliumlibeliumlibelium";

// Define a 32-Byte (AES-256) private key to encrypt message
//char password[] = "libeliumlibeliumlibeliumlibelium";

void setup()
{
  // put your setup code here, to run once:
  USB.ON();
  // set RTC on
  RTC.ON();

  frame.setID( mote_ID );

  //USB.print(F("message:"));
  //USB.println(message);
  //USB.println();

  //USB.print(F("public_exponent:"));
  //USB.println(public_exponent);
  //USB.println();

  //USB.println(F("public_modulus:"));
  //RSA.printMessage(modulus);
  //USB.println();

  // init XBee
  xbee802.ON();

}
```

```
void loop()
{
  //Show the remaining battery level
  USB.print(F("Battery Level: "));
  USB.print(PWR.getBatteryLevel(), DEC);
  USB.print(F(" %"));

  //Show the battery Volts
  USB.print(F(" | Battery (Volts): "));
  USB.print(PWR.getBatteryVolts());
  USB.println(F(" V"));
  delay(200);

  // put your main code here, to run repeatedly:
  val = analogRead(ANALOG3);
  delay(200);
  //USB.println(val);
  //if ((val < 250))
  //{
  //  USB.println(" "); // si las vibraciones son menores a los 500 manda un espacio en blanco
  // }
  //if ((val >= 300) & (val <= 500))
  //{
  // USB.println("Movimiento Leve"); // si las vibraciones son mayores a los 500 y menores a los 700 manda un mensaje
  //}
  //if ((val >= 600) & (val <= 800))
  //{
  // USB.println("Movimiento Medio"); // si las vibraciones son mayores a los 710 y menores a los 1000 manda un mensaje
  //}
  //if ((val >= 900))
  //{
  USB.println("Movimiento Fuerte !Alerta!"); // si las vibraciones son mayores a los 1000 manda un mensaje
  //c = c + 1;
  //USB.println(c);
  //if (c == 10)
```

```
// {
// c = 0;

frame.createFrame(ASCII, "SISMO S02");
USB.println(F("new Waspmote Frame created"));
frame.showFrame();
frame.encryptFrame( AES_192, password );
frame.showFrame();

// Calculating encrypted message
// RSA.encrypt(message
  //, public_exponent
  //, modulus
  //, enc_message
  //, sizeof(enc_message));

  //USB.println(F("-------------------------"));
  //USB.println(F("Encrypted message:"));
  //USB.println(F("-------------------------"));
  //RSA.printMessage(enc_message);
  //USB.println(F("-------------------------"));

  //USB.println(F("-------------------------"));
  //USB.print(F("Encrypted length:"));
  //USB.println((int)strlen(enc_message));
  //USB.println(F("-------------------------"));
  //USB.println();


//////////////////////////////////////////
// 2. Send packet
//////////////////////////////////////////

// send XBee packet
error = xbee802.send( RX_ADDRESS, frame.buffer, frame.length );
//error = xbee802.send( RX_ADDRESS, enc_message );

// check TX flag
if ( error == 0 )
{
```

```
    USB.println(F("send ok"));

    // blink green LED
    Utils.blinkGreenLED();
  }
  else
  {
    USB.println(F("send error"));

    // blink red LED
    Utils.blinkRedLED();
  }

  // wait for five seconds
  delay(50);
    //}
 // }
}
```

Anexo B: Muestra piloto

> textog=c(80.2, 77.2, 83.2, 74.6, 78.4, 77.1, 74.5, 76.8, 79.7, 75.7, 77.3, 75.4, 79.4, 78.7, 76.1, 75.4, 75, 75.3, 79.3, 76.2, 76.8, 78.4, 74.9, 77.2, 79.7, 77.2, 77.6, 76.6, 77, 76.4)

> var(textog)

[1] 3.865299

>

> texto1r=c(79.7, 75, 79.9, 76, 74.8, 76.5, 77.7, 77.4, 78.3, 79.8, 75.3, 76.3, 78, 79.5, 79.1, 75.6, 78.5, 79.8, 75.1, 78.1, 75.1, 76.2, 77, 75.4, 77.5, 75.9, 78.1, 75.9, 78.9, 78.1)

> var(texto1r)

[1] 2.792471

>

> aes12g=c(79.3, 82.1, 81.6, 77.6, 78.4, 77.3, 78, 80, 77.7, 80, 78, 77.4, 81.4, 78.5, 78.4, 80.3, 77.7, 82.4, 77.6, 81.4, 79.3, 80.4, 77.9, 79, 79.6, 77.2, 78.6, 81.4,79, 81.2)

> var(aes12g)

[1] 2.553345

>

> aes128r=c(77, 78.5, 82.5, 79, 77.1, 77.9, 78.2, 81.3, 80.6, 79.3, 83, 81.2, 84.3, 85.1, 79.4, 81.5, 81.4, 80.2, 81.7, 82.2, 79.6, 80.7, 81, 81.1, 81.1, 77.6, 82, 78.4, 81.7, 79.7)

> var(aes128r)

[1] 4.032195

>

> aes19g=c(79.3, 77.7, 78.6, 79.2, 80.2, 78.9, 80.2, 80.9, 81.2, 80.7, 78, 78.8, 78, 79.4, 78.8, 79.9, 78.8, 79.7, 78.9, 79.9, 80.6, 78.5, 79.8, 79.7, 80.3, 81.4, 80.3, 79.8, 81.1, 80.3)

> var(aes19g)

[1] 0.9835517

>

> aes192r=c(78.5, 76.6, 77.3, 78.3 ,77.7, 81.8, 81, 78.6, 77.6, 80.7, 79.1, 83, 78, 78.7, 79.4, 79.2, 81.1, 80.1, 79.9, 78, 81.5, 79.5, 77.6, 79.2, 80.5, 78.8, 81.5, 80.5, 81.4, 79.4)

> var(aes192r)

[1] 2.443506

>

> aes25g=c(78.1, 76.1, 77.8, 79.7, 75.4, 78.9, 78.3, 79.2, 78.7, 78.5, 77.3, 78.5, 75.7, 78.2, 76.5, 77.5, 76.1, 79.4, 79.8, 77.4, 77.3, 77.8, 77.9, 77.4, 76.3, 75.9, 79.8, 75.2, 77.4, 78.5)

> var(aes25g)

[1] 1.761195

>

> aes256r=c(79.2, 76.1, 79.6, 76.5, 78.4, 77.4, 74.5, 75.9, 77.3, 78.7, 79.4, 78.7, 80, 76.6, 78.8, 76, 76.9, 79, 77.3, 79.3, 75.5, 78.8, 78, 79.8, 75.4, 76.9, 78.5, 77.6, 78.6, 79.2)

> var(aes256r)

[1] 2.225161

>

> rsag=c(80.3, 80.4, 83.2, 81.6, 80, 86.9, 81.1, 80.3, 80.5, 80.9, 82.6, 81.4, 81.7, 82.1, 81.3, 80.9, 80.7, 83.1, 80.5, 82.3, 82.2, 80.5, 83, 81.6, 82.2, 81.4, 80.4, 81.2, 82.1, 82.4)

> var(rsag)

[1] 1.82823

>

> rsar=c(82.9, 81.3, 82.7, 82.7, 82.4, 83.1, 82.6, 83, 80.6, 80.6, 82.6, 82.3, 81.6, 81.2, 82.6, 81, 82.3, 82.7, 80.7, 81, 80.6, 80.6, 81.6, 82, 82.1, 82.7, 83.1, 81.6, 81.2, 82.8)

> var(rsar)

[1] 0.7562759

Anexo C: Mensajes enviados por los nodos sensores

- Texto Plano

  - Sensor 01: Sismo S01
  - Sensor 02: Sismo S02
  - Sensor 03: Sismo S03
  - Sensor 04: Sismo S04
  - Sensor 05: Sismo S05

- AES 128 (Longitud de la llave 16 bytes)

  - Sensor 01:
    `8_3g|TÍ+'KVmÃëk’7X¦‹ÛåÁ_ÛÀVí;^,EÕ£tÜô8éb¨ž¶X•ó«Œ1G

  - Sensor 02:
    `8_3g|TÍ+'KVmÃëk’7X¦‹Ûr,.²wbX¤j×R¨¿Üô8éb¨ž¶X•ó«Œ1G

  - Sensor 03:
    `8_3g|TÍ+'KVmÃëk’7X¦‹Ûå=oµ47Ë"P×ôëÜô8éb¨ž¶X•ó«Œ1G

  - Sensor 04:
    `8_3g|TÍ+'KVmÃëk’7X¦‹Û*ƒ*—&êu[R†ŽU˜HÞayÜô8éb¨ž¶X•ó«Œ1G

  - Sensor 05:
    `8_3g|TÍ+'KVmÃëk’7X¦‹ÛªíOåw»“é`¬Ào¡¹-Üô8éb¨ž¶X•ó«Œ1G

- AES 192 (Longitud de la llave 24 bytes)

  - Sensor 01:
    `8_3g|T"/V4u² ÍÄ°dÆHRòü3!¿ñûÏÞ;¦`Ô„<=ŸMÎ ìç{.ûqé{O3

  - Sensor 02:
    `8_3g|T"/V4u² ÍÄ°dÆHRòüá!”¾*…€ìyðÛ»±kgMÎìç{.ûqé{O3

  - Sensor 03:
    `8_3g|T"/V4u² ÍÄ°dÆHRòüå£Y‚‹†‚‡KD ·MÎìç{.ûqé{O3

  - Sensor 04:
    `8_3g|T"/V4u² ÍÄ°dÆHRòü–õ…¢!Æ*ƒ*ÊÑ‚íi[“°MÎìç{.ûqé{O3

  - Sensor 05:
    `8_3g|T"/V4u² ÍÄ°dÆHRòüIÜdƒ('ÇôþdoèSFMÎìç{.ûqé{O3

- AES 256 (Longitud de la llave 32 bytes)
    - Sensor 01:
      `8_3g|TfÃDÄÚ¹%@Äôö,çGÁ…ŒÚ¥ÊÁ€u¦¿SB□·ÖŒhñÓèµ…1]áÓ£þ¶
    - Sensor 02:
      `8_3g|TfÃDÄÚ¹%@Äôö,çGÁ…3nQÊƒ°ª¹Â={¥º‘·ÖŒhñÓèµ…1]áÓ£þ¶
    - Sensor 03:
      `8_3g|TfÃDÄÚ¹%@Äôö,çGÁw”ƒ¿²)íı»¥$ÿ°Õ‘·ÖŒhñÓèµ…1]áÓ£þ¶
    - Sensor 04:
      `8_3g|TfÃDÄÚ¹%@Äôö,çGÁ -§¡âÎ*ÃÏm&Ï„"·ÖŒhñÓèµ…1]áÓ£þ¶
    - Sensor 05:

      `8_3g|TfÃDÄÚ¹%@Äôö,çGÁî•Ð’)•/«GfJØmŸl0uO»>¥³5û9Qyq}

- RSA
    - Sensor 01:

      03AF7D8D31BD94F4957DC3F7776F1D73
      A54B367E7D9B311A31CBD7B0AB4FEEEE
      8A1C20F69DB1DE49D975211B00F8E746
    - Sensor 02:

      391B81B9F534ADD2F5391AECD6C285D2
      452A0F128A9B8D498D1C911205A00A3F
      E2AE0DD27ADE4C7AAB090CB2735A8186
    - Sensor 03:

      43A3520D001D76CC39221E6E316F9652
      4C6AD92D1965F73CCF6BC9424210AB8F
      C4A3AAAF26767ADC8169D08F6970436D
    - Sensor 04:

      131CDB07BBC25F5BC01B85B7069990DE
      E73FF2D4BED5DA412B7FC01BFB587ACA
      04B1863BD044E7FF068523FEB2399259

- Sensor 05:

  66F7F90220B0B198CF80A3C23CC44476
  1D2C8C08164D35B028BE62FEAE8EE59C
  B22D3693D212E34442A266FDD4D7C1C3