RAE

1.TIPO DE DOCUMENTO: Trabajo de grado para optar por el título de INGENIERO ELECTRONICO

2. TÍTULO: ANALIZADOR DE TRAFICO ZIGBEE

3. AUTORES: Leonardo Andres Sanchez Cuellar y Wesly Yardane Villamil Villamil

4. LUGAR: Bogotá, D.C

5. FECHA: Julio de 2021

6. PALABRAS CLAVE: Throughput, retardo, analizador de tráfico, estándar IEEE 802.15.4, ancho de banda, comandos AT, xbee, Protocolo de control de transmisión, Toolbox smart rf protocol packet sniffer, LaunchPad CC1352R, wireshark, Matlab.

7. DESCRIPCIÓN DEL TRABAJO: El objetivo principal de este proyecto desarrollar un analizador de tráfico ZigBee que permita la captura del tráfico y la generación de las métricas: throughput y retardo que permita dar solución a la problemática que se presenta en el semillero de convergencia tecnológica (No poder medir el tráfico que circulan por los estándares IEEE 802.15.4) y que pretende dejar un presente para futuros proyectos relacionados con el protocolo ZigBee; todo lo anterior basado en estudios anteriores de diferentes autores sobre los diferentes medios de captura del tráfico.

8. LÍNEAS DE INVESTIGACION: Línea de Investigacion de la USB: SolSytec. semillero de Convergencia tecnológica.

9. METODOLOGÍA: Es de carácter ingenieril, costa de 3 etapas; etapa de diseño, implementación y validación.

CONCLUSIONES: El proyecto ATRAZ ha encontrado una solución alternativa a hardware existentes que se disponen para la captura del tráfico del protocolo Zigbee. En el mercado los hardware desarrollados alcanzan precios muy altos y aun así cuentan con grandes limitaciones relacionadas a la frecuencia, No obstante, gracias a la solución de hardware implementada en el proyecto ATRAZ es posible explorar las bandas de 2.4 GHz y también bandas de frecuencia Sub-1GHz (Las bandas de 895 MHz y 915 MHZ), lo que lo vuelve un analizador completo en cuanto a Zigbee se refiere.

Las pruebas realizadas en el proyecto PIICO permiten identificar tramos en los que la señal no es perfectamente regular, al ser una red que envía datos periódicamente, no

debería ocurrir, sin embargo, gracias al análisis de tráfico realizado es posible identificar que si bien no es una pérdida de información dañina si es posible solucionarla adoptando un envío de paquetes redundante para garantizar el envió del 100% de la información.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

ANALIZADOR DE TRÁFICO ZIGBEE

Investigadores Semilleristas Grupo Solsytec

Sánchez Cuellar Leandro Andrés

Villamil Wesly Yardane

Tutor

Johana Carolina Martínez Ballesteros

UNIVERSIDAD DE SAN BUENAVENTURA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BOGOTÁ D.C.

2021

ANALIZADOR DE TRAFICO ZIGBEE.

Investigadores Semilleristas Grupo Solsytec

Leandro Andrés Sánchez Cuellar

Wesly Yardane Villamil

Tutor

Johana Carolina Martínez Ballesteros

Informe Final de Investigación

Proyecto FI 008_010

UNIVERSIDAD DE SAN BUENAVENTURA, SEDE BOGOTÁ

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

BOGOTÁ D.C.

2021

AGRADECIMIENTOS

En la ejecución de este proyecto queremos dar especial agradecimiento a Wilder Eduardo Castellanos que pensó primeros en nosotros antes que, en nadie para la realización de este proyecto, a la querida profesora Johana Carolina Martínez Ballesteros, que nos acogió cuando nos encontrábamos desamparados sin tutor, nos quiso lo suficiente y nos tuvo la suficiente paciencia para no regañarnos (demasiado), A nuestros amigos y familia por su apoyo incondicional.

Contenido

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

INTRODUCCIÓN

Con el auge que está teniendo el internet de las cosas y con el surgimiento de nuevas tecnologías y protocolos de comunicación en la actualidad, estas últimas han adquirido un grado de complejidad importante. Con esto, surge una necesidad y es que actualmente hacen falta herramientas que permitan analizar ciertas métricas y de esta manera poder evaluar el rendimiento de la red en cuestión.

Con el antecedente previamente establecido, el proyecto ATRAZ busca desarrollar una herramienta para analizar el tráfico que circula por una red Zigbee, pues hoy en día es uno de los protocolos más usados en el área de la investigación, ya que tiene características como bajo consumo de energía y buena distancia de cobertura, esto lo hace un protocolo atractivo para trabajar.

Las métricas como el throughput, el retardo y el número de paquetes perdidos en muchas ocasiones son datos de interés para el usuario que busca evaluar el desempeño su red; con ATRAZ el usuario tendrá una herramienta capaz de conseguir las métricas para conocer y mejorar el rendimiento en su red, lo cual es el propósito de esta investigación de semillero.

.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

1. PLANTEAMIENTO DEL PROBLEMA.

La masificación de dispositivos electrónicos que requieren transmitir información, por ejemplo dispositivos como sensores, enrutadores, nodos de procesamiento de datos, entre otros; ha llevado a la creación de nuevas reglas y protocolos para establecer la comunicación entre ellos [1][2]. Estos nuevos protocolos, generalmente para establecer comunicación inalámbrica, tienen sus propias características desde el punto de vista funcional así como desde el punto de visto técnico. Por ejemplo la mayoría de los protocolos pensados para Internet de las cosas (IoT, Internet of Things, por sus siglas en inglés), se caracterizan por un menor consumo de recursos y un menor tráfico de control [3], [4], lo que los hace adecuados para ser instalados en pequeños dispositivos de recursos computacionales limitados. Esta variedad de protocolos hace compleja, no solo la interacción entre dispositivos, sino también el análisis del funcionamiento y el rendimiento de las conexiones establecidas. Esto surge principalmente debido a que la adopción de nuevos protocolos es más rápida que la generación de las herramientas esenciales para su análisis razón por la cual, en la actualidad las herramientas que capturan el tráfico están diseñadas a ciertas frecuencias y están fijas, lo que resulta difícil al momento de acoplarlas sobre la red de sensores al igual que el software que implementa el capturador. Por otra parte, el protocolo IEEE 802.15.4 es uno de los más utilizados en la actualidad para la implementación de redes de sensores y en la construcción de escenarios con IoT, por ejemplo, en el sistema PIICO, que es una plataforma de IoT que se ha desarrollado dentro del grupo de investigación Solsytec de la Universidad de San Buenaventura, sede Bogotá. En general, en las redes Zigbee, los dispositivos y elementos de la red, intercambian mensajes de manera inalámbrica, pero este tipo de redes no cuentan con una herramienta que permita analizar el tráfico y determinar posibles fallos o la cantidad de información perdida. A partir de lo expuesto anteriormente, se formula la siguiente pregunta problema para orientar la investigación que se propone: ¿Cómo evaluar el desempeño de una red ZigBee a partir del análisis del tráfico que circula por ella?

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

2. ANTECEDENTES

El surgimiento de nuevos protocolos de comunicación genera consigo la necesidad de analizar los parámetros más importantes del tráfico de estos mismos, ZigBee es uno de los protocolos más utilizados de la actualidad. Se destaca por ser un protocolo inalámbrico, de amplia cobertura, facilidad de configuración y bajo consumo energético, que aunque se lleva desarrollando desde el año 2003 [10] puede considerarse bastante reciente y se apunta a que su implementación se verá incrementada en los años venideros, como lo fue en principio el diseño e implementación de comunicación ZigBee basado en un sustrato para redes de sensores inalámbricos del 2006 una fecha en la cual ZigBee a penas se estaba dando a conocer, y Li & Chou quisieron ir más allá montando una red de sensores inalámbricos de Wireless Sensor Network (WSN) [5], que provee una gran cantidad de nodos de sensores conectándolos simultáneamente sin embargo, al no ser producidos por el mismo proveedor se necesitaba un estándar de comunicación para interconectarlos, con la menor perdida de información posible.

En un WSN basada en Zigbee, varios dispositivos pueden enviar datos periódicamente, por lo cual requiere un algoritmo que permita evitar que se pierdan o se confundan los datos es por ello que se implementa en la capa de red de ZigBee un algoritmo para disminuir este caso. Tomando en cuenta que un nodo Zigbee puede manejar roles en el nodo estos pueden ser: coordinador, enrutador o dispositivo final, esto trae algunos problemas al momento de enviar tramas si no se escoge la topología o los nodos , en dado caso Li & Chou [5] propone dar prioridad a los objetos a seguir, buscar nodos con más rapidez , obviamente este proceso requiere más tiempo ya que debe asociarse con el nuevo nodo y así sucesivamente, no obstante se puede utilizar la unión huérfana y tener el mismo resultado , esto permite que el objeto se una al enrutador, convirtiéndose en el hijo del enrutador y así todos los enrutadores pueden enviar paquetes al coordinador (Para especificar qué objeto está en el rango del enrutador), finalmente para evitar el problema de encontrar un nodo oculto o que no se esté utilizando , la capa de

red Zigbee se le incrusta un TxOffset con valores en la carga útil de una baliza, que indican las diferencias de tiempo entre la baliza y sus vecinas. Al considerar los valores de TxOffset, un algoritmo de programación de balizas puede evitar el problema de los nodos ocultos.

El desarrollo e investigación sobre analizadores de tráfico para Zigbee son escasos pero valiosos para este proyecto, Un artículo publicado en el año 2007 realizó el análisis de trafico de una red Zigbee en presencia de redes WLAN [6], lo cual es ciertamente interesante pues Zigbee comparte con otros protocolos el rango de frecuencia de los 2.4 GHz, por lo tanto, es un detalle a tener en cuenta, dado que en la mayoría de los casos otras redes siempre serán motivos de interferencia significativos.

Se ha estudiado el efecto de la interferencia mutua en el rendimiento de las redes WLAN y ZigBee. Sikora y Groza [7] midieron los efectos de WLAN, Bluetooth, ZigBee y Microhorno en la pérdida de paquetes o cuadros de cada sistema con equipos de la vida real en diversos entornos. Kim y col. [8] midió el efecto de los dispositivos WLAN y un Microhorno en el rendimiento de la tasa de error de trama (FER) de los dispositivos ZigBee para variar un canal ZigBee operativo y la distancia entre un transmisor ZigBee y un receptor ZigBee. Shuaib y col. [9] también midió el efecto de WLAN y ZigBee en el rendimiento de cada sistema en diversos entornos.

Howitt y Gutiérrez [10] analizaron el impacto de la coexistencia de la red ZigBee en dispositivos WLAN considerando un área de interferencia efectiva. Se han realizado estudios sobre algoritmos de coexistencia entre redes WLAN y ZigBee. Kang y col. [11] midió el efecto de la interferencia WLAN en los dispositivos ZigBee y propuso un algoritmo de coexistencia reactiva basado en un concepto de agrupamiento. Jung y col.[12] propuso un algoritmo de coexistencia proactiva. En este algoritmo, un dispositivo que tiene módulos WLAN y ZigBee arbitra la transmisión del tráfico WLAN y ZigBee.

Teniendo en cuenta como los datos son afectados por los nodos o topologías, Xuo en el 2010 plantea el diseño e implementación de una red inalámbrica de sensores para hogares inteligentes[13], el cual abarco todo el tema de nodos y como estos son los encargados de recolectar toda la información dependiendo el tipo de topología que utilicen , teniendo en cuenta ahora los protocolos de comunicación, para lo cual es necesario buscar los sensores adecuados que permitan realizar la interacción entre estos mismo, asumiendo con base al mismo protocolo de comunicación para luego poder encontrar la ruta más corta u óptima posible en él envió de tramas de paquetes al módulo central ZigBee, proporcionando una solución de enrutamiento factible para sistemas domésticos inteligentes.

Consecutivamente los mismos autores publicaron un nuevo artículo en el que se realizaba del mismo modo el análisis de tráfico del protocolo Zigbee, esta vez en presencia de interferencia Bluetooth, ambos trabajos se encuentran fuertemente relacionados, sin embargo, en este caso existe un enfoque más específico al estudio de la interferencia generada por un protocolo tan popular como lo es Bluetooth. En este artículo, los autores analizan el funcionamiento de los dispositivos ZigBee en presencia de interferencia Bluetooth y formulan un modelo matemático para analizar el rendimiento de una red ZigBee. [14]

De Serbia surge un documento en el que se habla a detalle de un Software creado para analizar el rendimiento de una red Zigbee en cursos universitarios [15]. Este estudio es relevante para esta investigación porque por primera vez se habla de un software de análisis de tráfico, aunque carece de la profundidad de los modelos matemáticos encontrados en los documentos de Chong previamente estudiados. No obstante, este documento permite orientar para realizar el desarrollo de un software más completo.

Zigbee es un protocolo que se vuelve cada vez más popular por sus características, una de ellas es el bajo consumo, pero también es importante resaltar que en el espectro,

Zigbee maneja diferentes rangos de frecuencia, más específicamente los rangos de 2.4 GHz, 784 MHz, 868 MHz y 915 MHz siendo el rango de frecuencia más comúnmente usado el de los 2.4 GHz, esto ha generado que se realicen múltiples investigaciones centradas en este único rango de frecuencia y que el desarrollo de dispositivos se limite a realizar la captura en este rango. Se han desarrollado algunos dispositivos que pueden realizar la captura de otros rangos de frecuencia para Zigbee, no obstante, estas soluciones a nivel de hardware por lo general alcanzan valores muy altos en la industria haciéndolos poco accesibles.[16]

Posteriormente en el 2017, Luo diseño todo un sistema inteligente de hogar basado en ZigBee [17] y SIP el cual llevo más allá la red inalámbrica de Xu [13], el cual plantea la relación costo-beneficio. Además, utiliza un proveedor de servicios SIP para enviar los datos obtenidos hacia la nube y hacia el celular, esto lo logra definiendo la seguridad del sistema al pasar de direcciones IPv4 a IPv6 por su amplio espectro de direcciones y estructurando una topología de conexión p2p (la cual verifica la IP de la dirección con la del teléfono al cual se piensa conectar los diferentes sistemas) se lleva a cabo por medio de la puerta de enlace, encargada de verificar la identidad con el SIP , esta escucha la petición del teléfono y verifica el registro de la puerta de enlace, vinculando o emparejando los comandos del teléfono con el dispositivo ZigBee.

Recientemente, en el año 2019, la compañía Texas Instruments sacó el módulo CC1352R SimpleLink™ High-Performance Multi-Band Wireless el cual permite, mediante el software Smart RF Packet sniffer tambien de Texas Instruments, poder enlazar el módulo con el computador mediante puerto micro USB, lo que garantiza que este software pueda vincularse a una interfaz gráfica externa y poder observar los distintos tráficos que circulan.[18]

3. JUSTIFICACIÓN

El protocolo de comunicación ZigBee tiene unas características que lo convierten en un importante componente en los nuevos sistemas de interconexión de dispositivos básicamente, por ser fácilmente implementable y por su bajo consumo de recursos en términos de CPU y memoria. Numerosas aplicaciones de IoT han sido desarrollados recientemente con ZigBee. Por ejemplo, en la integración de este protocolo con otros como WiFi y Bluetooth [19] en la implementación de soluciones IoT para el hogar [20] y para industria[21]. Lo anterior muestra lo valioso que es desarrollar herramientas que faciliten el trabajar con dicho protocolo.

Esta propuesta de investigación está centrada en la solución de una necesidad real que se tiene en la Plataforma para la Interoperabilidad de Internet de las Cosas - PIICO y en general, en las redes ZigBee y es la falta de una herramienta para analizar el desempeño de la red. Con la solución desarrollada en este proyecto se podrán realizar los análisis necesarios para determinar el nivel de desempeño de las comunicaciones por el protocolo ZigBee esto permitirá tener resultados más confiables haciendo que el material destinado a difusión tenga un mejor nivel.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

4. OBJETIVOS

Para solucionar esta necesidad, se planteó un objetivo general el cual fue desglosado en tres objetivos específicos que llevan a su cumplimiento y que se encuentran a continuación.

4.1 Objetivo general.

Desarrollar un analizador de tráfico ZigBee que permita la captura del tráfico y la generación de las métricas: throughput y retardo.

4.2 Objetivos específicos.

- Identificar los componentes necesarios para la construcción de un analizador de tráfico para redes Zigbee.
- Desarrollar el analizador de tráfico y la programación de la aplicación software que permita la generación de las métricas necesarias para determinar el rendimiento de la red.
- Evaluar la herramienta desarrollada mediante la captura y análisis de tráfico ZigBee.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

5 MARCO CONCEPTUAL.

En el diseño e implementación de una red inalámbrica se deben plantear la mejor relación costo- beneficio, por lo que un sistema basado en ZigBee puede aportar un bajo nivel de consumo energético y una transmisión de datos baja, perfecta para enviar pequeños tramos de información con el menor gasto energético posible [17] además, es necesario conocer el número de nodos a trabajar, el tipo de red al cual se va a enlazar el sistema, el software de almacenamiento para los datos recolectados y el hardware que permita recolectar dichos nodos[13], como cualquier sistema, este posee pérdidas , ya que, al tratarse de una gran cantidad de nodos y sensores conectados simultáneamente, pueden existir colisiones de paquetes, esto sumado a que cada sensor empleado puede no ser producido por el mismo proveedor, es por esto que se necesita un estándar de comunicación para interconectarlos con la menor perdida de información posible[5], una solución a este problema es poder enlazar todos los datos obtenidos en un hardware, el cual a través del software valide y muestre el flujo de datos y paquetes perdidos, ayudando al usuario en la visualización del rendimiento (throughput) mediante el GUI y como mejorarlo en el sistema implementado.

Posteriormente se deben mirar qué tipos de nodos se van a trabajar, recordando que un nodo está compuesto principalmente por varios sensores y un módulo inalámbrico ZigBee [13]. En la industria, los nodos se pueden implementar en una red con una topología en forma de estrella, malla o híbrida. En el área de monitoreo, los nodos ZigBee están esparcidos con una distancia entre todos y todos estos envían datos del sensor al coordinador de la red a través de la red. Un nodo Zigbee puede manejar roles en el nodo, estos pueden ser: coordinador, enrutador o dispositivo final. [5]Cuando el rol es de coordinador, este verifica si el nodo está en una red ZigBee para esto utiliza 4 pasos para verificar este estado: Primero, recibe la solicitud de la capa de aplicación y genera una exploración de energía buscando el nodo con menor energía de señal para intentar formar una WPAN en ese canal. Segundo, de acuerdo con el nivel de energía en el

nodo, este realiza el procedimiento de exploración pasiva, en el cual el nodo busca un ID de PAN disponible para conectarse. Tercero, recibe la información de la MAC, el nodo ingresa una solicitud de inicio a la MAC, la cual se encargará de programar la transmisión periódica de datos. Finalmente, cuando se recibe la confirmación de la solicitud de inicio, el nodo ingresa como coordinador de estado. El rol de enrutador es explorar todos los canales disponibles y devolver la información PAN a los canales, de acuerdo con la información se elige un PAN al cual se pretende unir y emite la solicitud de emparejamiento. Posteriormente la capa de red selecciona el nodo con más intensidad de señal en el PAN y lo asocia con la capa MAC.[5]

Una vez se implemente una red Zigbee con todos los parámetros, es necesario verificar qué tan eficaz es esta red ante diversos escenarios (variación de las distancias de nodos, diferentes sensores) y así mismo mirar que capturadores en la actualidad hay que permitan observar el tráfico, caso específico el Módulo Inalámbrico Zigbee CC 2531 que trabaja a 2.4GHz en el estándar IEEE 802.15.4 el cual es necesario flashear con un debugger para poder descargar el firmware, descargar los archivos necesarios para generar un archivo .exe , posteriormente descargar las dependencias que se necesitan de acuerdo a lo que se requiera; se descarga cualquier herramienta que permita leer y visualizar los paquetes a través del módulo como por ejemplo WireShark , todos estos pasos generan muchos inconvenientes para las personas que no saben o no conocen del tema, es por ello que se da la solución de hacer un entorno amigable al usuario por medio de una interfaz gráfica de usuario, el cual evita que el usuario tenga que realizar descargas, flasheos, instalaciones de programas externos y dependencias, todo es concentrado en un solo software capaz de mover la interfaz por medio del capturador y mostrar las gráficas pertinentes que ayudaran a buscar rápidamente posibles fallos en una red nodos.

Por tal motivo y como necesidad para prever futuras inconsistencias de una red ZigBee, se planteó la solución de crear una interfaz con el usuario capaz de observar en tiempo

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

real la cantidad de tráfico que pasa a través de un nodo cualquiera y la cantidad de paquetes perdidos, con estos datos obtenidos se puede realizar un estudio de toda la red ZigBee que servirá como base para replantear la red de tal modo que haya mayor rendimiento a través del canal de comunicación y así mismo poder utilizar la aplicación en cualquier otra red .

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

6 METODOLOGÍA.

A continuación, se describe la metodología para el desarrollo del trabajo de investigación y el desarrollo del proyecto. La metodología se encuentra basada en un modelo clásico de diseño ingenieril el cual destaca por estar dividido en tres etapas de diseño, implementación y validación como se aprecia en la Figura 1.

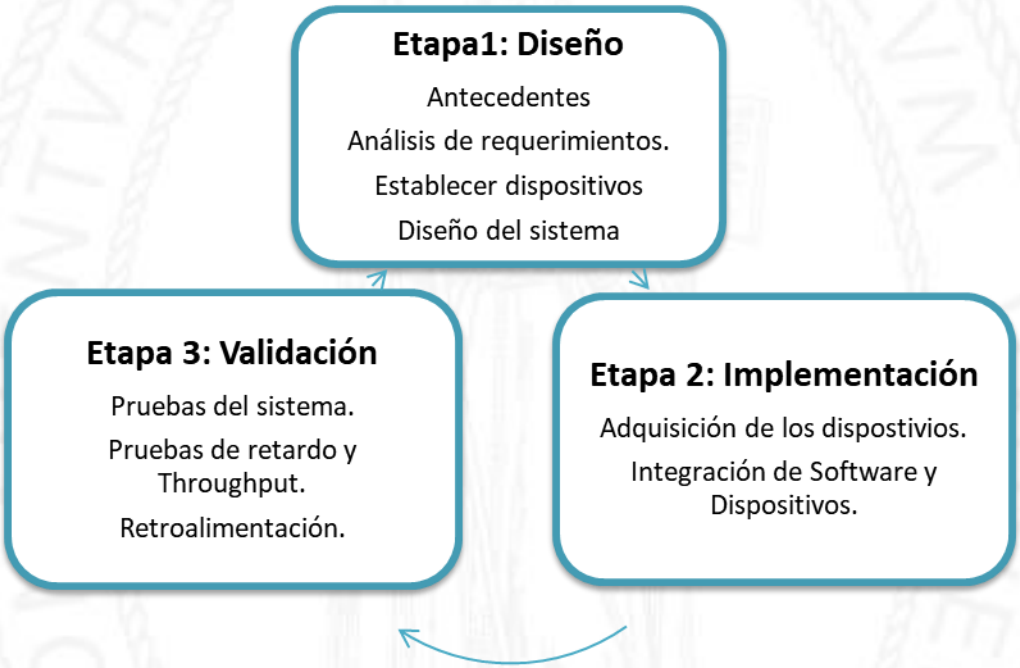

Figura 1. Desarrollo del proyecto en etapas de diseño ingenieril.[22]

El proyecto se desarrolla en 3 etapas: la primera etapa es el diseño, en donde se elabora el análisis de los antecedentes y referentes de la temática que se trabaja, se realiza un diseño preliminar del sistema de captura de tráfico y se selecciona el hardware necesario.

En la segunda etapa: se hace una implementación del prototipo, la cual consiste en realizar la adquisición de equipos, la integración en una misma plataforma y la programación de estos.

Finalmente, en la etapa 3, se hace la validación del sistema implementado en la que se realizarán diferentes experimentos para aprobar su funcionamiento tales como: pruebas de retardo pérdida de paquetes y throughput, con el fin de establecer el comportamiento y el rendimiento de la plataforma implementada. La metodología completa se segmenta en diferentes etapas, tal como se observa en la Figura 2.

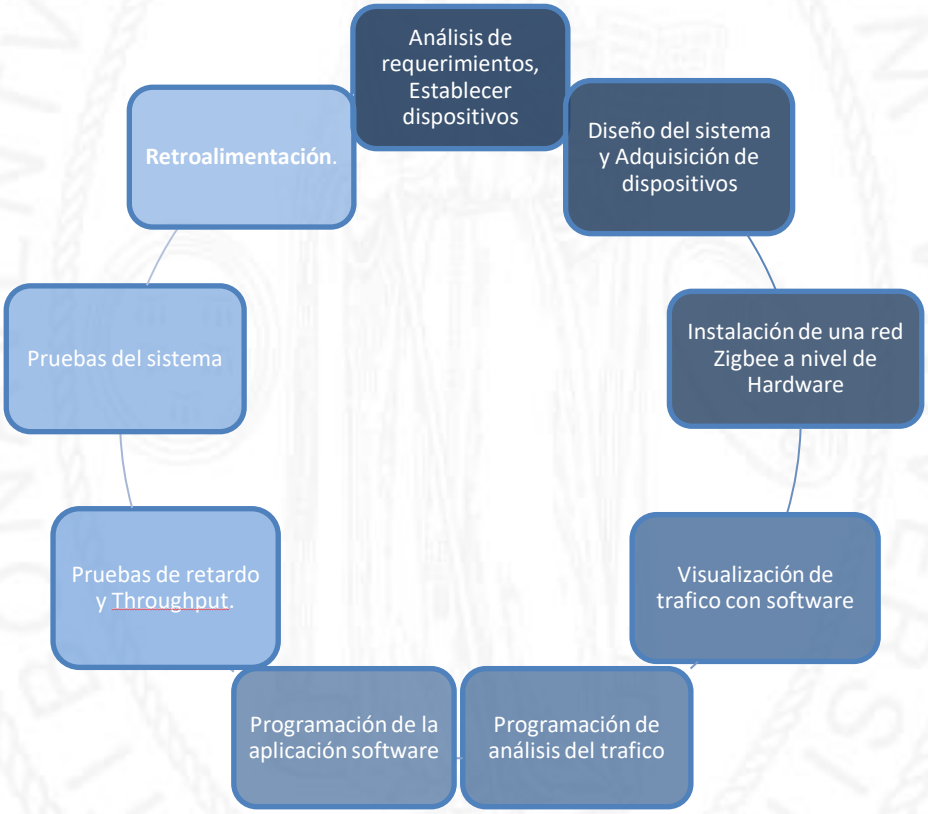

Figura 2. Metodología completa[22]

En este proceso, se planteó dar inicio con el análisis de requerimientos y el establecimiento de los dispositivos necesarios, para luego realizar el diseño del sistema y se adquieren los dispositivos, después se hizo la instalación de una red Zigbee a nivel de Hardware, para posteriormente conseguir la visualización del tráfico con el software.

Se realizó la programación del análisis del tráfico, utilizando una interfaz gráfica de usuario y una vez logrado lo anterior se hacen las primeras pruebas de retardo y Throughput, para finalmente realizar las pruebas del sistema con la retroalimentación por si hay que hacer un ajuste necesario.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

7 CARACTERISTICAS DE ZIGBEE

Para entender el funcionamiento del sniffer con el protocolo IEEE 802.15.4 es necesario conocer cómo trabaja ZIGBEE internamente, así se logra entender cada una de sus tramas, topologías, arquitectura, tipos y capas, todo esto con el fin de que se permita entender una manera más fácil el protocolo y como este llega a funcionar como sniffer. De esta manera es posible encontrarse en contexto de que es lo que se encontrará al momento de realizar el análisis del tráfico del protocolo Zigbee.

Teniendo en cuenta lo anterior, se procede a detallar las características referentes al protocolo Zigbee como lo son las capas, sus topologías y la estructura de las tramas con las cuales trabaja.

7.1 Capa Zigbee.

El protocolo ZigBee está determinado por la capa física y la capa MAC según el estándar IEEE 802.15.4 las capas superiores de este protocolo están conformadas por la capa de Framework de aplicación y de red también llamada pila ZigBee. En la última, la capa de aplicación se ha dado la posibilidad de que el usuario pueda hacer desarrollo basado sobre el protocolo y además se ha implementado un Framework cuya función es la interoperabilidad entre los fabricantes [23].

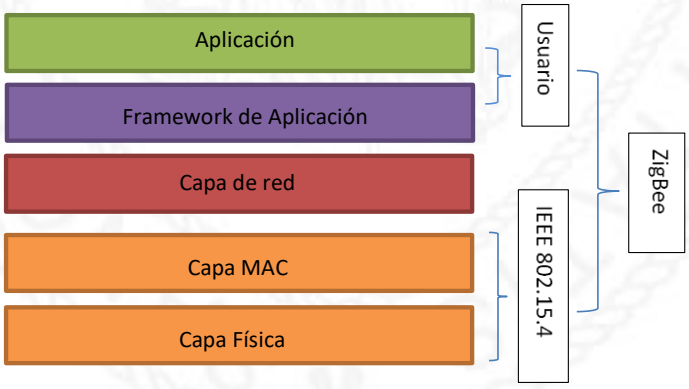

Figura 3. Modelo de pila ZigBee.[24]

ZigBee concreta todo su protocolo de red en el aire relativamente ya que deja implementar el desarrollo de APIs (Interfaz de programación de la aplicación) a los vendedores y fabricantes de estos productos lo cual para el desarrollador conlleva en especificar el vendedor con el protocolo del dispositivo ZigBee, dado que cada uno tiene un estándar para aprobar el protocolo [25]. Para crear una red del tipo ZigBee se debe tener presente los tres tipos de roles en los dispositivos:

Dispositivo coordinador: El cual se encarga de crear la red de sensores y enlazar los routers y dispositivos finales, solo existe uno por cada red WPAN [26].

Dispositivo router: Ayuda a enrutar los paquetes entre los nodos de la red.

Dispositivo final: Son dispositivos que se enlazan con los periféricos, estos solo envían y reciben información. [27]

7.2 Topología Zigbee.

Una vez se haya elegido el tipo de red que manejara los dispositivos ZigBee, se forma la topología, se pueden conformar tres tipos, una de ellas es la topología estrella, la cual el nodo coordinador es el encargado de enlazar todos los dispositivos. En la topología malla, se mantiene un coordinador, sin embargo, el enlace se puede ejecutar entre dispositivos que sean del mismo rango y que se pueda adaptar para extender el alcance de la red, permitiendo la posibilidad de tener enlaces redundantes. Finalmente, la topología tipo árbol en la cual el coordinador mantiene la sincronización con las derivaciones de los enlaces en la red.[23]

Algunos desarrolladores implementan en sus sistemas de domótica fabricantes de transceptores como Texas Instruments[28][29] o como uno de los líderes del mercado:

Digi. El cual se basa en los dispositivos XBEE PRO S2B, que han sido muy usados en el árdea de la domótica, dentro de este desarrollo existen dos tipos de modos; El modo transparente permite que los datos sean enviados sin ninguna trama y con trasmisión tipo broadcast, como los presentados en los trabajos de[30][21][26]. El otro modo es el API, en el cual Digi [31] ha implementado un Framework que permite reconfigurar de manera remota sus dispositivos, generar envíos unicast desde la trama y revelar los dispositivos conectados a la red, todo esto, establecido en una trama definida por este fabricante, facilitando acceso completo a todas las características del protocolo ZigBee.

El modo API se ha perfeccionado por los trabajos presentados en [32][33] Este uso del modo API de XBEE consiente en aprovechar la capacidad de enrutamiento del protocolo con la reconfiguración y actualización de los dispositivos de forma manual. Asimismo, mientras el modo transparente requiere que el desarrollador este a cargo en el procesamiento el uso del modo API permite que el mismo firmware que está establecido de fabrica realice el procesamiento.

7.3 Tipos de tráfico Zigbee.

Las aplicaciones que se llevan a cabo en ZigBee tienen un tráfico que puede catalogarse en uno de los siguientes tipos:

a) Datos periódicos (continuo): La aplicación limita una tasa de datos en un tiempo determinado por esta misma. Un caso típico es donde un sensor necesita transmitir la temperatura cada 10 segundos.[27]

b) Datos intermitentes (por eventos): En este caso la aplicación junto a otras aplicaciones, programas o sensores externos al dispositivo definen la tasa de datos. Como, por ejemplo, en un sistema domótico, los interruptores de luces envían datos solo ante un

cambio de posición. En tanto estén desconectados (comúnmente) consumiendo una energía mínima. [27]

c) Datos periódicos con comunicación garantizada (GTS) (Guaranteed Time Slot): Existen aplicaciones de baja latencia que necesitan comunicación libre por el canal. GTS es un método de calidad de servicio que garantiza la atención por diferencia de tiempo, delta de t (Δt) dentro de un período T llamada Super trama. El estándar IEEE 802.15.4 proporciona un modo de trabajo denominado “con baliza” que se usa como multiplexación temporal. [27]

7.3.1 Tipos de dispositivos

Dentro del estándar IEEE 802.15.4 se definen dos tipos de dispositivos con el objeto de minimizar el costo en el sistema:

a) Full Function Device (FFD): Son dispositivos idóneos para funcionar en cualquier topología, alcanzan a ser coordinadores o coordinadores de red. Capaz de dialogar con cualquier otro.

b) Reduced Function Device (RFD): Solo funciona con los miembros de una red en topología estrella y solo pueden conversar con el coordinador de red, estos dispositivos son de bajo requerimiento, complejidad, procesamiento y de memoria.[27]

7.3.2 Arquitectura ZigBee

El estándar ZigBee está compuesto por unos protocolos o conjuntos de bloques, más conocido como Capas, cada una independiente de la otra. Cada capa ejecuta una función única para la capa que se localiza en su nivel superior.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Los estándares IEEE 802.15.4 y ZigBee se complementan suministrando un modelo de capas de protocolos como la que se ilustra a continuación en la figura 4:[34]

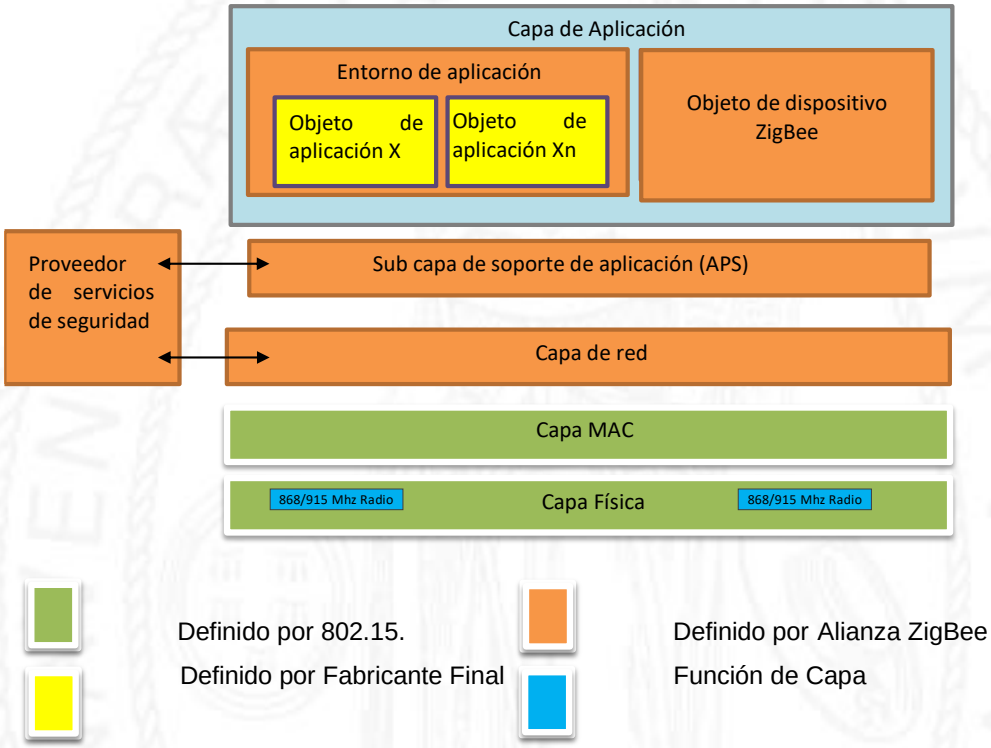

Figura 4. Capas que conforman la pila de protocolos para ZigBee [7].

7.4 Tramas del protocolo Zigbee

La estructura de una trama del protocolo Zigbee viene dada por una serie de al menos seis bytes de los cuales cada uno cumple una serie de propósitos a la hora de identificar y analizar un mensaje.

Como se puede observar en la Figura 5 el primer byte consiste en un encabezado el cual permite identificar el inicio de una trama, este byte será 0x7E para cualquier trama

entrante. Los dos bytes siguientes están para definir la longitud del mensaje, posteriormente irán los datos incluidos en la trama misma, correspondientes a su estructura API (Necesaria durante una comunicación) esta información puede ir desde el byte 4 hasta un byte n y por último, el byte final es un comprobante de que la trama ha llegado a su fin.

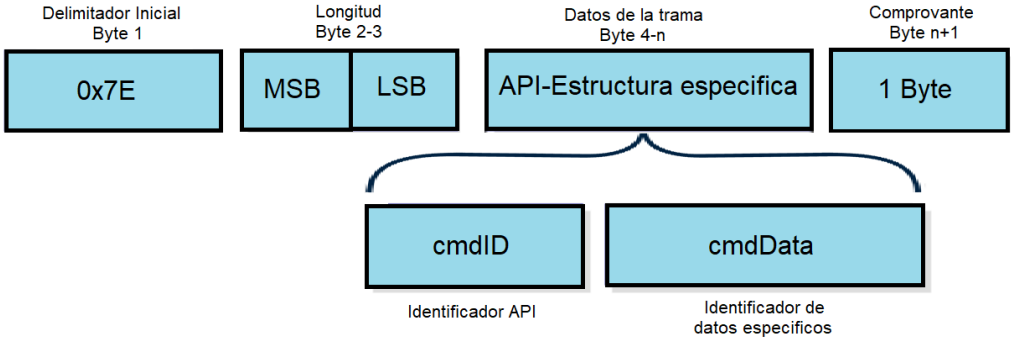

Figura 5. Estructura de una trama básica API [35]

Entre tramas puede existir un espaciado de tiempo el cual puede ser corto o un extenso, en el protocolo Zigbee es importante tener en cuenta estos dos datos debido a que de esta manera será sencillo identificar cuando la trama esta seguida de ACK (Protocolo de control de transmisión) tal como se observa en la Figura 6.

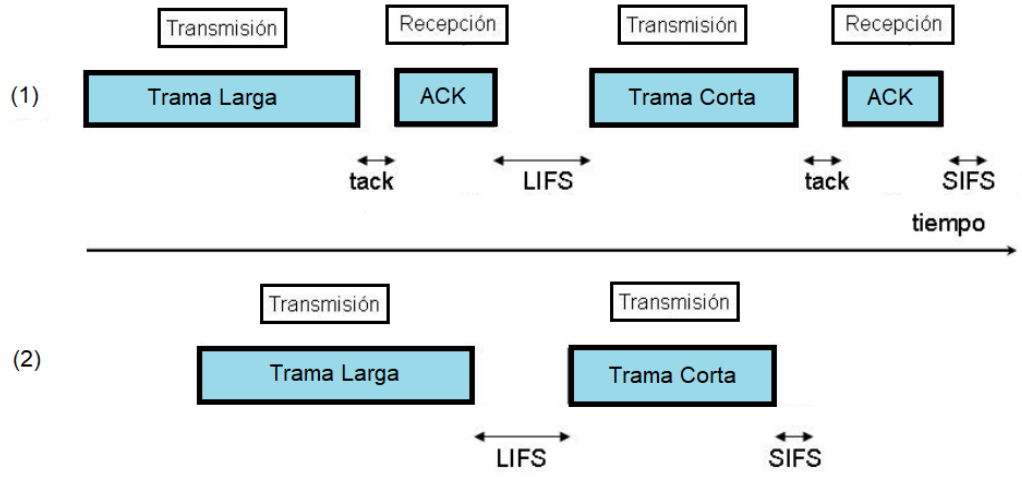

Figura 6. Espaciado entre tramas: (1) Con presencia de ACK. (2) Sin presencia de ACK. [35]

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

7.4.1 Comando at del módulo Xbee

El modo comando permite integrar comandos AT al módulo Xbee, para entrar en este modo es necesario utilizar el programa XCTU, algún microcontrolador con UART o desde el mismo hyperterminal de Windows, los comandos AT permiten conocer de manera alternativa la configuración de los XBEE, ajustar o modificar parámetros, así como cambiar su modo de operación, entre otros.

El comando básico para poder entrar en el modo AT está definido por un tiempo dado con el comando GT (Guard Time, o ATGT = 0x3E85 que equivale a 1000ms) luego se ingresa +++ y se esperar un tiempo GT, la respuesta de este módulo debe ser OK.

El módulo Xbee viene por defecto con una velocidad de 9600bps. En caso de no poder ingresar al modo de comandos, puede que se deba a la diferencia de velocidades entre el módulo y la interfaz que se comunica vía serial. Cada comando AT posee una Sintaxis la cual permite el uso correcto de la interfaz.

Prefijo “AT”	Comando ASCII	Espacio (opcional)	Parámetro (HEX)	Carrier<return>
AT	DL		1F	<CR>

Figura 7.Sintaxis de un comando AT.[36]

En la figura anterior, se muestra la sintaxis de un comando AT. Luego de entrar a este modo, se debe ingresar el comando deseado para ajustar los parámetros del módulo Xbee. La lista de comandos de encuentra en las siguientes secciones. A continuación, se encuentra la Tabla 1, la cual presenta un listado de comandos At con los que es posible realizar configuraciones de los módulos y hacer preguntas sobre el estado actual de configuración, siendo posible llevar a cabo comunicaciones entre dos módulos Xbee como se observa a lo largo de subsección

Tabla 1. Lista de comando AT(Tomado de [37])

Comando	Sintaxis	Función	Predeterminado
+++	+++	Pasar a modo de comando en línea (no precedido de AT)	
/	/	Pausa (no precedido de AT)	125 ms
A	ATA	Responder manualmente	
A/	A/	Repetir el último comando (no precedido de AT)	
D	ATD	Marcado n Nº de teléfono, de 0 a 9	
DT	ATDT	T Marcado por tonos	
DP	ATDP	P Marcado por pulsos	
DTWn@	ATDTWn@	@ Esperar respuesta (X3, X4)	
DTn!n	ATDTn!n	! Indicar conexión	
DTn#n	ATDTn#n	# Dígito auxiliar de marcado por tonos	
DTn,n	ATDTn,n	, Pausa de marcado (S8)	2 segundos
DTn"n	ATDTn"n	Establezca el modo textual para lo siguiente:	
D$	ATD$	Mostrar una lista de comandos de marcado	
DL	ATDL	Repetir el último número marcado	
DL?	ATDL?	Mostrar el último número marcado	
DSn	ATDSn	Marcar el número almacenado	
E0	ATE0	Desactivar eco de comandos (echo off)	
E1	ATE1	Activar eco de comandos (echo on)	X
F0	ATF0	Activar eco en línea	
F1	ATF1	Desactivar eco en línea	X
H0	ATH0	Colgar (enlace activado)	
S$	ATS$	Mostrar la lista de valores de registros S	
Sr=n	ATSr=n	Cambiar registro S de "r" a "n"	

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Por ejemplo, si quiere comenzar desde el XCTU, se empieza vinculando el dispositivo Xbee mediante la configuración de consola con el comando AT, seguido de un tiempo de espera de 1000ms para proceder a escribir +++ e inicializar los comandos, lo cual hará que el módulo responda con un 4F 4B 0D o un OK como se observa en la Figura 8.

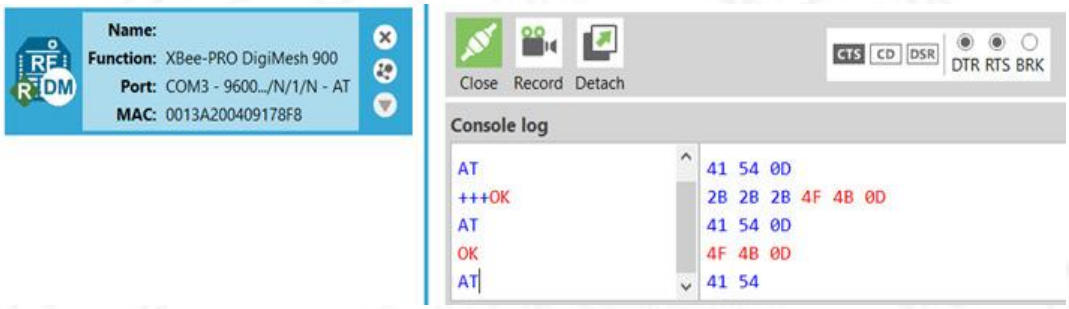

Figura 8. Introducción a los comandos AT desde XCTU[22]

Una vez se establece la comunicación, se procede a escribir instrucciones de acuerdo con la sintaxis de comandos AT; por ejemplo, escribir el último número marcado con el comando ATDL o dirección de destino, En caso de no haber escrito alguna orden, se espera por parte del módulo un FFFF, lo que se evidencia en la figura 9.

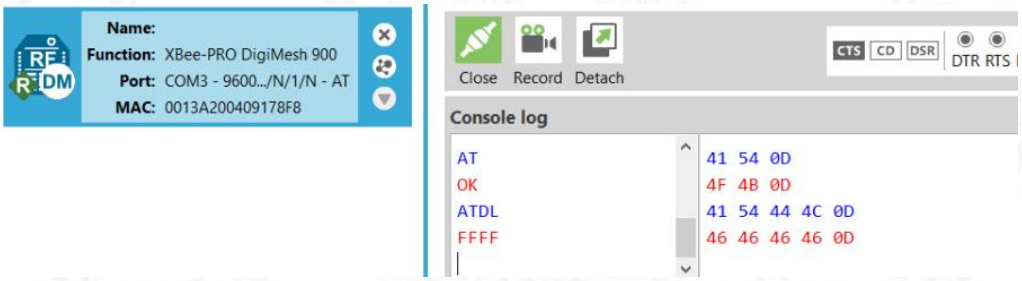

Figura 9. Comando ATDL con respuesta[22]

También se puede pregunta por la dirección de destino alta (ATDH), para lo cual se tiene como respuesta la dirección 0x0 y poder guardar estos datos en la memoria no volátil con el comando ATWR (Figura 10).

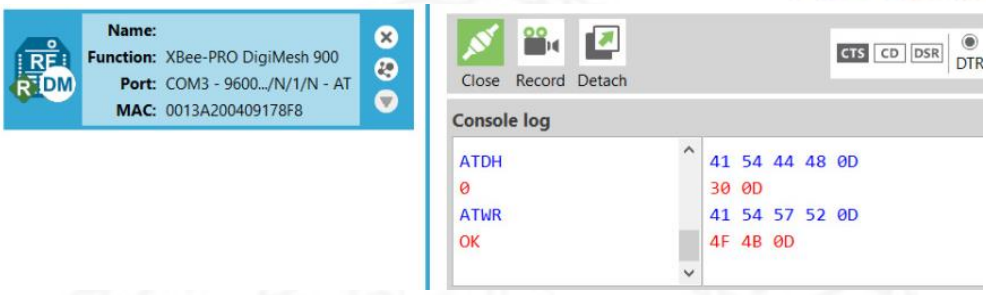

Figura 10. Configuración no volátil de la memoria y dirección de destino alta.[22]

8 NECESIDADES Y PROPUESTAS DE SOLUCIÓN

Como ya se ha venido trabajando a lo largo de este documento, un analizador de tráfico es una herramienta cuyo principal objetivo es el de capturar las tramas de una red. Es un error pensar que un analizador de tráfico o Sniffer de red como es también conocido (del verbo Sniff que significa olfatear) es una herramienta de software la cual se puede realizar en su totalidad con código. Esto es un error debido a que a pesar de que es posible contar con herramientas de software que permiten realizar el análisis del tráfico de redes de área local, es solo debido a que los equipos en los que se ejecutan dichos análisis cuentan con las características de hardware para capturar dicho tráfico. Las herramientas de este tipo se limitan a realizar la captura de los protocolos más populares y de uso más comercial como por ejemplo Bluetooth y WiFi, no obstante, al momento de contemplar otras posibilidades como el protocolo Zigbee serán extremadamente escasas las computadoras que cuenten con receptores Zigbee debido a la poca implementación de éste en el mercado actual.

Con la contextualización expuesta anteriormente es correcto a firmar que un analizador de tráfico es una herramienta tanto de software como de hardware, este último representa una función de gran importancia sin el cual el análisis de tráfico será sencillamente imposible de realizar, pues su tarea es encargarse de realizar la captura y

la recepción de las tramas capturadas y la parte de software se encargará de realizar la visualización y el análisis respectivo.

8.1 Requisitos de hardware y dispositivos.

A continuación, se listan una serie de dispositivos que son necesarios para realizar un entorno de análisis de tráfico, algunos elementos deben cumplir las tareas de generar una red mediante el protocolo Zigbee y otros, requieren una serie de características adicionales para que cumplan funciones de sniffing.

CC2531 - Analizador Usb Dongle sniffer 2.4GHz

El CC2531 (Figura 11), es un sistema en chip (SoC) por puerto USB para aplicaciones IEEE 802.15.4, ZigBee y RF4CE, combina el transceptor de RF con un MCU 8051, con una memoria flash programable en el sistema, 8 KB de RAM también tiene códigos fuente para las bibliotecas USB HID y CDC , el transceptor de RF es compatible con IEEE 802.15.4 de 2.4 GHz, maneja una potencia de salida programable hasta 4,5 dBm y en caso de utilizar redes asíncronas solo se necesita un único cristal ,opera con el protocolo USB 2.0 (12 Mbps).

Figura 11. Modulo CC 2531 Sniffer 2.4 GHz.[38]

Modulo CC1352R – SimpleLink

El dispositivo SimpleLink ™ CC1352R es un microcontrolador (MCU) multiprotocolo y multibanda (Sub-1 GHz y 2.4 GHz) compatible con el protocolo Zigbee, Bluetooth 5.1 Low Energy, IEEE 802.15.4g, objetos inteligentes habilitados para IPv6 (6LoWPAN) , MIOTY, sistemas patentados, incluido el TI 15.4-Stack (Sub-1 GHz y 2.4 GHz), y multiprotocolo concurrente a través de un controlador Dynamic Multiprotocol Manager (DMM), el cual se presenta en la Figura 12.
El dispositivo está optimizado para comunicaciones inalámbricas de baja potencia y detección avanzada en los mercados de sistemas de seguridad de edificios, HVAC, medidores inteligentes, redes médicas, cableadas, electrónica portátil, cine en casa y entretenimiento y periféricos conectados.

Este LaunchPad no es propiamente un Sniffer, sin embargo, es posible realizarle algunas modificaciones, en su mayoría a través de programación, con las cuales se puede adaptar para que cumpla funciones de sniffing.

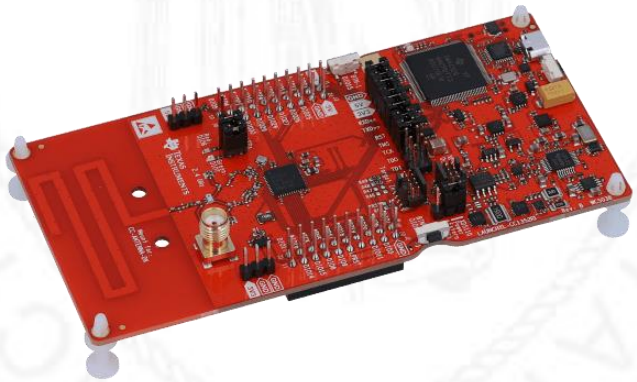

Figura 12. Modulo Cc1352R – SimpleLink de Texas Instruments. [39]

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Modulo Xbee

Los módulos Xbee son pequeños radios que pueden comunicarse de manera inalámbrica y que funcionan principalmente para conectarse mediante el protocolo Zigbee y derivados del mismo como por ejemplo Digi-Mesh. Estos módulos son fácilmente configurables y existen diferentes variedades con características que varían entre sí. Estos módulos se conectan de manera serial a un computador y pueden trabajar mediante el CMD del equipo o por el software propiedad de Digi XCTU.

Estos módulos permiten entablar una comunicación en el protocolo Zigbee y mediante estos generar un entorno de comunicación para ser analizado (Figura 13).

Figura 13. Módulos de radio frecuencia (RF) Digi XBee[40]

Adaptador Xbee serial / usb

El adaptador Xbee permite que su funcionamiento se base en la conversión USB a serial (UART), donde las líneas seriales van conectadas a las del Xbee. Es capaz de operar con los módulos los módulos Xbee Standar y Xbee Pro y solo necesario conectar el módulo en la base y conectar el cable USB, de esta manera se tiene acceso a los pines seriales para operación y configuración del módulo. Desde el puerto micro USB a USB.

Cuenta con una salida dual de voltaje DC de 3.3v y 5v, opera el protocolo USB 2.0 (velocidad hasta 12 Mbps) y unas dimensiones de 3.8cm X 2.5cm lo cual la hace compacta para los diferentes entornos (Figura 14).

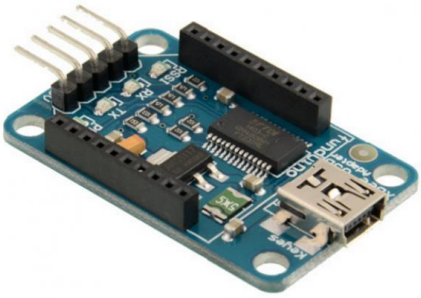

Figura 14. Adaptador Xbee serial / usb[40]

Acople de antena a modulo Xbee-09 Pro

Antena con frecuencia de resonancia de 900MHz Hembra con conector RP_SMA, con una longitud: 17cm y 19.5cm desde la base en la línea un diámetro de 1.2cm y un peso de 27 gramos (Figura 15). La ganancia es de 3.5 dbi lo cual permite que sea idónea para trabajar en el área que se pretende medir.

Figura 15. Acople de antena hembra a modulo Xbee-09 pro[41]

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

8.2 Escenarios de aplicación del proyecto ATRAZ

Como se presentó en la metodología, para desarrollar un analizador de tráfico en el protocolo Zigbee la prioridad será tener un entorno para analizar. Es por este motivo que se han contemplado tres escenarios diferentes para garantizar que la captura de tráfico sea universal. Los escenarios de prueba para la realización del proyecto son en su totalidad entornos controlados de comunicación en el protocolo Zigbee cuyas diferencias se encuentran en las aplicaciones que desempeñan y la frecuencia en la que se transmiten los paquetes.

8.2.1 Proyecto PIICO/S-PIICO

El proyecto PIICO es un proyecto de investigación dentro de la universidad de San Buenaventura asociado al semillero de investigación Solsytec dentro del que se encuentra el proyecto ATRAZ.

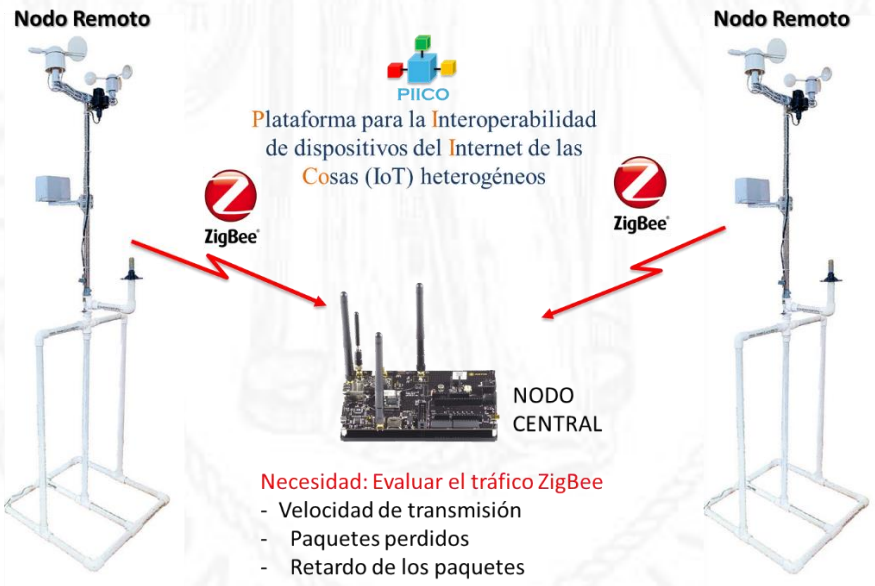

Figura 16. Escenario de prueba Proyecto PIICO [42]

El proyecto PIICO a grandes rasgos, es una plataforma en la que se miden una serie de variables ambientales que se transmiten entre un nodo central encargado del

procesamiento de los datos y dos nodos remotos encargados del censado de las variables. La particularidad de este proyecto es que uno de los protocolos utilizados para realizar la comunicación es el protocolo Zigbee por lo cual se vuelve un escenario de prueba perfecto, En la Figura 16. se ve de manera conceptual el funcionamiento de proyecto PIICO.

8.2.1 Comunicación con módulos Xbee 09 PRO a 915MHz

El segundo escenario de pruebas consta de una comunicación sencilla que se puede identificar como punto a punto en la que se realiza un intercambio de paquetes mediante dos módulos Xbee 09-PRO configurados mediante el entorno de DIGI XCTU el cual es un software con compatibilidad total con los módulos Xbee y el cual ofrece un entorno amigable y fácil de trabajar, tal como se presenta en la Figura 17.

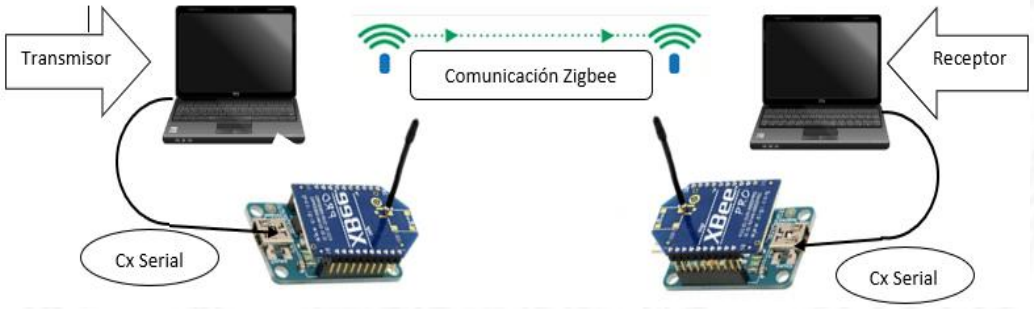

Figura 17. Esquema de comunicación ZigBee [22]

8.2.2 Implementación del TI LaunchPad LPSTK-CC1352R

El kit LaunchPad SensorTag LPSTK-CC1352R de Texas Instruments cuenta con una gran variedad de sensores ambientales y con la tecnología SimpleLink que lo convierte en un dispositivo de fácil implementación (Figura 18).

Figura 18. LaunchPad de Texas Instruments LPSTK-CC1352R[43]

Además. cuenta con compatibilidad con varios protocolos entre los que destaca el Zigbee y opera bandas de frecuencia de 2.4 GHz y frecuencias Sub GHz. Por lo que sirve para un escenario adicional de pruebas de captura de tramas en el protocolo Zigbee.

9 DESARROLLO DE HERAMIENTA PARA ANALISIS DE TRÁFIO ZIGBEE.

Al momento de diseñar un sniffer capaz de trabajar con múltiples frecuencias y acoplarse a un proyecto ya estipulado es necesario primero buscar y comparar los elementos necesarios para realizar el correcto aprovechamiento de recursos y eficiencia del sistema, es por esta razón, que dentro del desarrollo de esta sección se encontrarán diversas tablas comparativas que sustenten las decisiones para elegir dispositivos como el software necesario en la implantación del analizador.

9.1 Dispositivos

Para llevar a cabo la construcción del analizador de tráfico En el protocolo Zigbee se tuvieron en cuenta una serie de dispositivos que cumplían los requisitos para funcionar

como Sniffers de red. Después de una investigación profunda se descartaron varios de los dispositivos, algunos muy prometedores. Esto debido a sus altos costos pues oscilan entre los 300 y 500 dólares. No obstante, los dispositivos que más se adecuan a las necesidades del proyecto se redujeron a la mitad, El Launchpad de Texas Instruments CC1352R y el USB Dongle CC2531 también de Texas Instruments.

Como es posible apreciar en la Tabla 2, ambos dispositivos tienen características muy cercanas, aunque sin duda el Launchpad CC1352R supera al Modulo CC2531 en casi todo. Además de esto, el LaunchPad es una tarjeta multiprotocolo con la cual es posible innovar sobre el proyecto ATRAZ en el futuro, permitiendo trabajar en otros protocolos y otras frecuencias. Una característica en la que el CC2531 es inferior es en las frecuencias trabajadas, debido a que este módulo solo opera con la banda de frecuencia de 2.4 GHz, frecuencia que trabaja también el CC1352R, sin embargo, se destaca que el Launchpad también trabaja con frecuencias Sub-GHz.

Dado el análisis anterior, se pueden identificar las características que permiten el Launchpad CC1352R sobre el módulo CC2531; puesto que los dos dispositivos son accesibles en cuanto a precio y se encuentran dentro del presupuesto del proyecto, ciertamente el CC2531 es un tanto más económico, no obstante, las características expuestas en la Tabla 2. del CC1352R hacen que se justifique el gasto adicional, debido a que, además de cumplir con las necesidades del proyecto ATRAZ es una adquisición valiosa para el semillero convergencia tecnológica.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Tabla 2. Comparación de módulos para adquisición de datos Zigbee(Basado en las referencias de los fabricantes[44] *)*

Características	Módulo CC2531 Sniffer	Modulo Cc1352R - SimpleLink
Frecuencia de trabajo	2.4GHz	Sub-1 GHz --- 2.4GHz
Modo activo RX (CPU inactivo)	24 mA	24.9 mA
Rango de voltaje de alimentación	(2 V – 3.6 V)	(1.8- 3.8 v)
Núcleo de microcontrolador 8051 de alto	rendimiento y bajo consumo con código.	Núcleo Arm® Cortex-M0 de bajo consumo.
Flash programable en el sistema	256 KB o 128 KB	352KB
RAM	8KB retención en todos los modos de alimentación.	80KB ram
Periféricos	SI	SI
Frecuencia de trabajo	48M Hz	48MHz
ADC	12 bits con ocho canales y resolución configurable.	12 bits con ocho canales y resolución configurable.
UART	Dos, con soporte para varios protocolos seriales.	Tres, con soporte para varios protocolos seriales

Módulo Xbee 09-pro 900Mhz/Zigbee vs Xbee Zigbee S2C TH 2.4GHz

Los módulos Xbee son unos radios que se puede comunicar de forma inalámbrica unos con otros, reemplazando un par de cables en una comunicación serial, diseñado para una red de alto tráfico de datos, con baja latencia y una sincronización de comunicación

basada en el protocolo ZigBee IEEE 802.15.4, para una red Punto-Punto, Punto a Multi Punto, P2P. La comparación entre los módulos Xbee S2C, Xbee-Pro y Xbee 09-Pro se presenta en la Tabla 3.

Tabla 3. Comparación entre módulos Xbee(Tomado de [31]*)*

Especificación	Xbee S2C	Xbee-pro	Xbee 09-Pro
Rango Indoor	Hasta 30 metros	Hasta 100 metros	Hasta 300 metros
Rango Línea de vista	Hasta 100 metros	Hasta 1.5 kilómetros	Hasta 3 kilómetros
Potencia transmitida	1mW (0 dBm)	60 mW (18 dBm)	50mv(17 dBm)
Velocidad de RF	250Mps	250Mps	126Kbs
Velocidad de Interfaz serial	1.2Mps-115Mps	1.2Mps-115Mps	1.2Mps-115Mps
Sensibilidad Recibida	-92 dBm (1%perdida de paquetes)	-100 dBm (1%perdida de paquetes)	-100 dBm (1%perdida de paquetes)
Voltaje	2.8v-3.4v	2.8v-3.4v	3v-3.6v
Corriente transmitida	45mA (3.3 v)	Hasta 227 mA (3.3v)	210mA
Frecuencia de Operación	ISM 2.4 GHz	ISM 2.4 GHz	ISM 900 MHz
Topología Soportada	Punto-Punto, Punto a Multi Punto, P2P	Punto-Punto, Punto a Multi Punto, P2P	Punto-Punto, Punto a Multi Punto, P2P
Número de Canales	16	12	12

A pesar de que los módulos Xbee pro y S2c tienen unas muy buenas velocidades de transferencias por encima de los 200 Mb su alcance de cobertura es muy corto por lo

cual a la hora de montar una red física y pensando en el futuro del semillero se escoge el módulo Xbee 09 Pro que da un margen de hasta 300 metros y 3 km de rango en línea de vista, así mismo como los datos a enviar no son de gran volumen entra dentro del margen con sus 126Kps.

9.2 Toolbox smart rf protocol packet sniffer

Smart RF Packet Sniffer es herramienta en una aplicación desarrollada por Texas Instruments para computador, la cual permite almacenar y visualizar paquetes emitidos mediante un hardware de RF que se encarga escuchar. El dispositivo de captura se conecta mediante USB al computador y la herramienta es compatible con varios protocolos entre los que destaca Zigbee.

El Packet Sniffer es un toolbox que puede filtrar y decodificar los paquetes si se reprograma de esa manera y que permite verlos de una manera cómoda e intuitiva, como lo hacen herramientas consolidadas en el mercado como Wireshark y está disponible para dispositivos de las series CC13xx y CC26xx de Texas Instruments. En la Tabla 4 se realiza una recopilación de los protocolos con los que se puede trabajar en el software de Smart RF Packet Sniffer y los equipos que pueden realizar las labores de captura de tráfico para dichos protocolos. En amarillo se subrayan los equipos seleccionados para realizar el proyecto debido a su compatibilidad tanto con el software como con el protocolo.

En la Tabla 4. Es importante prestar especial atención en los protocolos Zigbee y RF4CE, este último debido a que sus fundamentos están basados en Zigbee por lo que podría ser una siguiente fase de investigación de proyectos venideros en la que se realicen análisis en protocolos basados en Zigbee como RF4CE o Digi Mesh.

Tabla 4. Compatibilidad de protocolos de Smart RF Packet Sniffer[18]

Protocol	Version	Capture device	Can be used to capture packets from
Bluetooth®	**Bluetooth core spec 4.0**	CC2540 USB Dongle	CC2540
low energy		CC2540EM+SmartRF05EB	CC2541 CC2640, CC2650 CC2642R, CC2652R CC1352R, CC1352P Bluetooth®
ZigBee	**2007/PRO 2006 2003**	CC2531 USB Dongle CC2530EM+SmartRF05EB CC2520EM+SmartRF05EB CC2430EM+SmartRF04EB/SmartRF05EB CC2431EM+SmartRF04EB/SmartRF05EB CC2430DB	CC2420 CC2430, CC2431 CC2480 CC2520 CC2530, CC2531 CC2630, CC2650 **CC2652R, CC1352R CC1352P[1]** ZigBee devices
	2003	CC2420EM+CC2400EB CC2420DB	ZigBee devices
RF4CE	**ZigBee RF4CE 1.0.1**	CC2531 USB Dongle CC2530EM+SmartRF05EB CC2520EM+SmartRF05EB CC2520EM+SmartRF TrxEB CC2430EM+SmartRF04EB/SmartRF05EB CC2431EM+SmartRF04EB/SmartRF05EB CC2430DB	CC2533 CC2530 CC2531 CC2620, CC2650 **CC2652R, CC1352R CC1352P[2]** ZigBee RF4CE devices

[1] Los datos resaltados en amarillo hacen referencia los dispositivos seleccionados para trabajar.

[2] Ibid.

Es por este motivo que la solucion de software y hardware dispuestos para realizar el analizador de tráfico han sido definidos como el software de Smart RF Packet Sniffer para hacer que un hardware cumpla con las funciones de análisis de tráfico y el TI LaunchPad LAUNCHXL-CC1352R que en circunstancias normales no es un hardware de sniffing, cumpla funciones de captura de tráfico con la ayuda de la reconfiguración de la tarjeta por medio de Packet Sniffer. Con esto los requerimientos a nivel de hardware están cumplidos, pues la tarjeta LauchPad CC1352R funciona como una antena que se conecta a cualquier equipo para capturar tráfico en las frecuencias que se manejan en el protocolo Zigbee, no obstante, hace falta un componente a nivel de software que realice el cálculo y visualización de las métricas obtenidas de esta captura para sacar conclusiones sobre el desempeño de las redes Zigbee que se estén analizando.

9.2.1 Toolbox smart rf protocol packet sniffer

Cuando se inicia por primera vez el software de Texas Instruments lo que se observa es una pequeña ventana llamada Smart RF Sniffer Agent, la cual se encarga de realizar el escaneo del dispositivo en el toolbox. En este caso el dispositivo seleccionado es el LaunchPad CC1352R de Texas instruments, pues pertenece a una familia de equipos compatibles y cumple con los requisitos de protocolo Zigbee y frecuencia de 2.4 GHz. La ventana se muestra en la Figura 19.

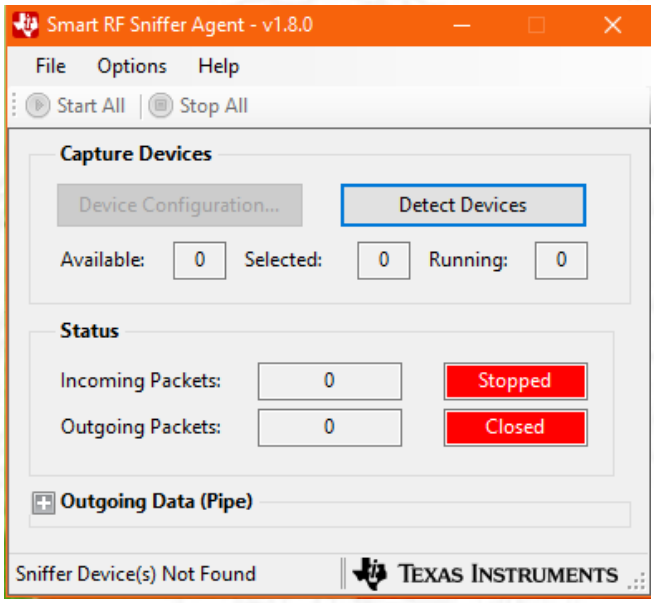

Figura 19. Entorno de Smart RF Packet Sniffer de Texas Instruments.[22]

El entorno del Smart RF Agent a simple vista no funcionara a no ser que sea reconocido por el equipo el cual se está ejecutando, para que el software de Texas instruments logre ser un receptor funcional deberá instalar los drivers automáticamente una vez se conecte. La figura 20 se muestra el reconocimiento del LaunchPad en el administrador de dispositivos.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

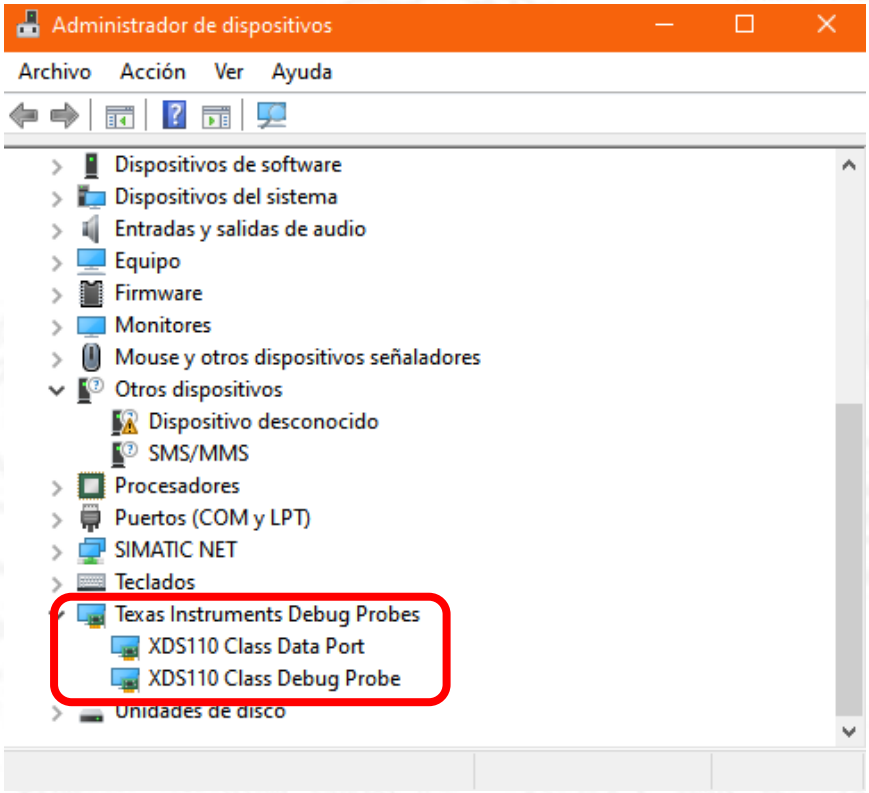

Figura 20. Tarjeta reconocida por el Administrador de dispositivos.[22]

Uniflash es la herramienta con la cual los dispositivos de Texas Instruments logran resetearse de manera correcta para que se ejecuten sin ningún problema, es por ello que en la Figura 21, se observa la interfaz del software UniFlash en el que se realiza una búsqueda en la librería de dispositivos compatibles, se puede buscar manualmente la LaunchPad CC1352R1o desde la opción Detect device, de esta manera se encargará de hacer un escaneo a los dispositivos conectados en busca de una referencia compatible.

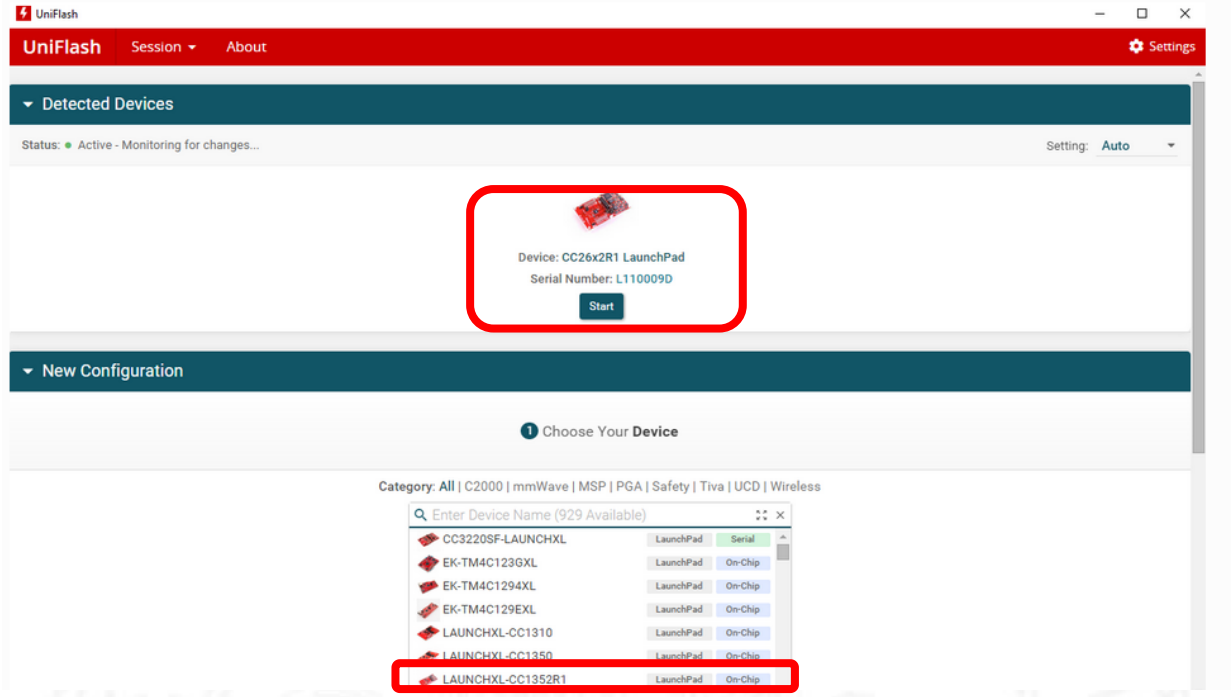

Figura 21. Selección de dispositivos en UniFlash para realizar la configuración de Sniffer.[22]

Cuando el dispositivo ha sido detectado, se ejecuta y se dirige a una nueva pestaña del software en la que se solicita cargar a la tarjeta, la imagen de la tarjeta correspondiente, esta imagen se encuentra en la dirección <install_path>\SmartRF Packet Sniffer 2\sniffer_fw\bin como se muestra en la Figura 22.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

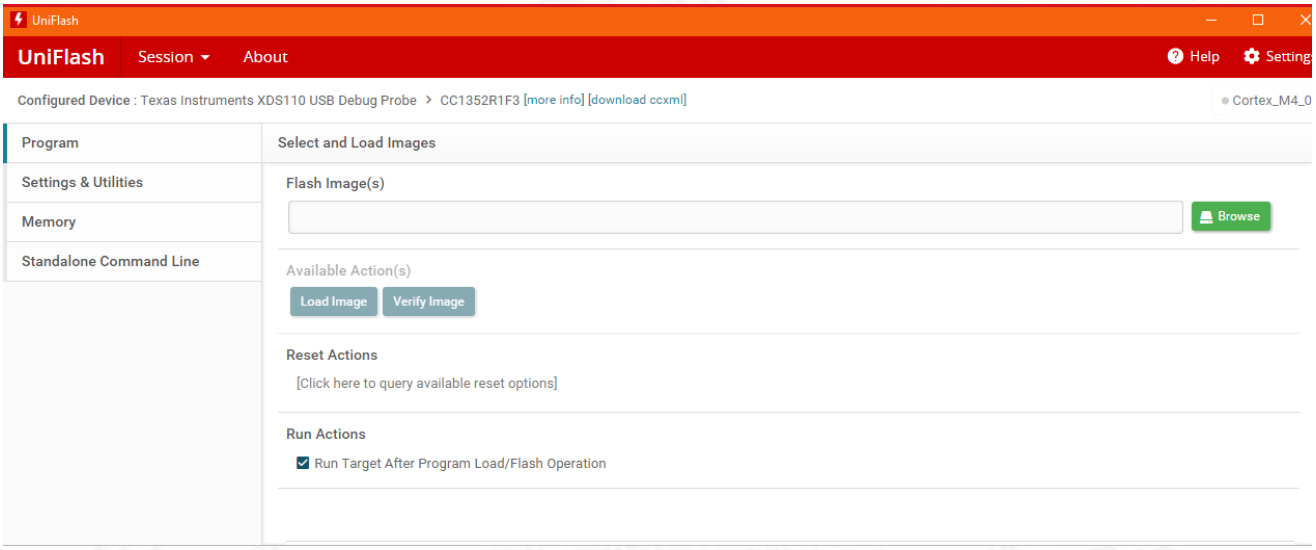

Figura 22. Carga de la imagen de la tarjeta para compatibilidad con Smart RF.[22]

Una vez realizado la carga de la imagen, el Smart RF Sniffer Agent estará listo para su uso. Es importante que todas las aplicaciones de Texas Instruments se encuentren cerradas para poder operar con normalidad.

Adentro de la aplicación de Smart RF, se selecciona uno de los modos de operación expuestos a continuación, los cuales servirán para generar el muestreo de tráfico desde la interfaz de Wireshark:

1. **Pipe (recomendado):** los datos se envían a Wireshark en la máquina local
2. **Socket (modo independiente):** los datos se envían al adaptador de bucle invertido de Microsoft con Wireshark ejecutándose en la máquina local.
3. **Socket (modo remoto):** los datos se envían a Wireshark en otra máquina o en la máquina local mediante el adaptador de red.

El modo utilizado fue el modo PIPE que es el recomendado así que desde Options > Data out se selecciona PIPE y luego OK como se observa en la siguiente Figura 23.

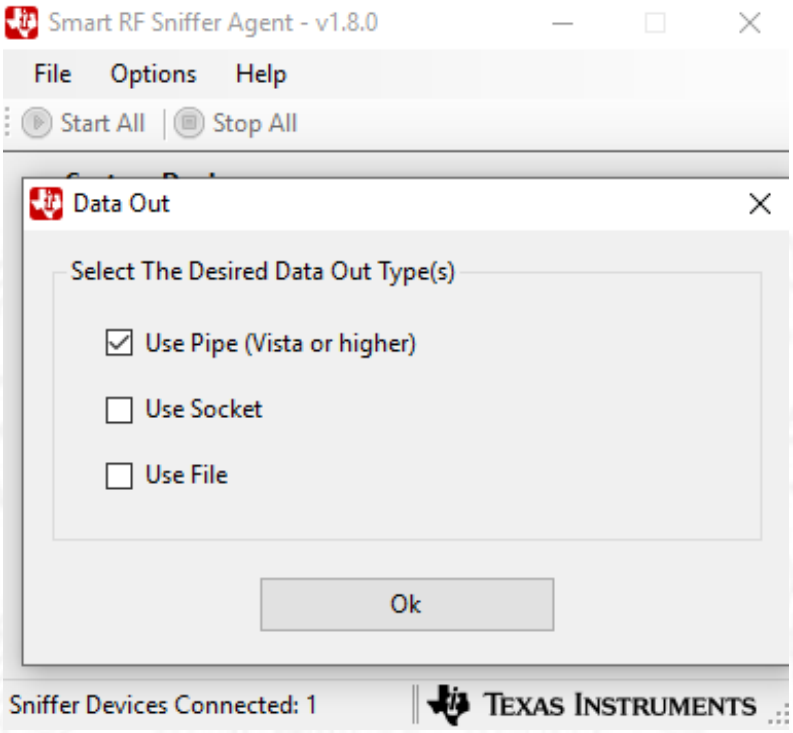

Figura 23. Selección de modo Pipe para realizar el vínculo con WireShark.[22]

Ahora ya es posible realizar la configuración de la tarjeta para seleccionar los protocolos a trabajar; se puede apreciar que, gracias a las características de la tarjeta seleccionada, es posible realizar la captura de Zigbee a más de una frecuencia, pues entre las opciones se encuentra el estándar IEEE 802.15.4 (Zigbee) en las frecuencias de 2.4 GHz, 915 MHz y 868 MHz por lo que todas las bandas de Zigbee están cubiertas con este dispositivo. En la Figura 24. Se observa la interfaz de Smart RF Packet Sniffer con el dispositivo configurado detectado.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

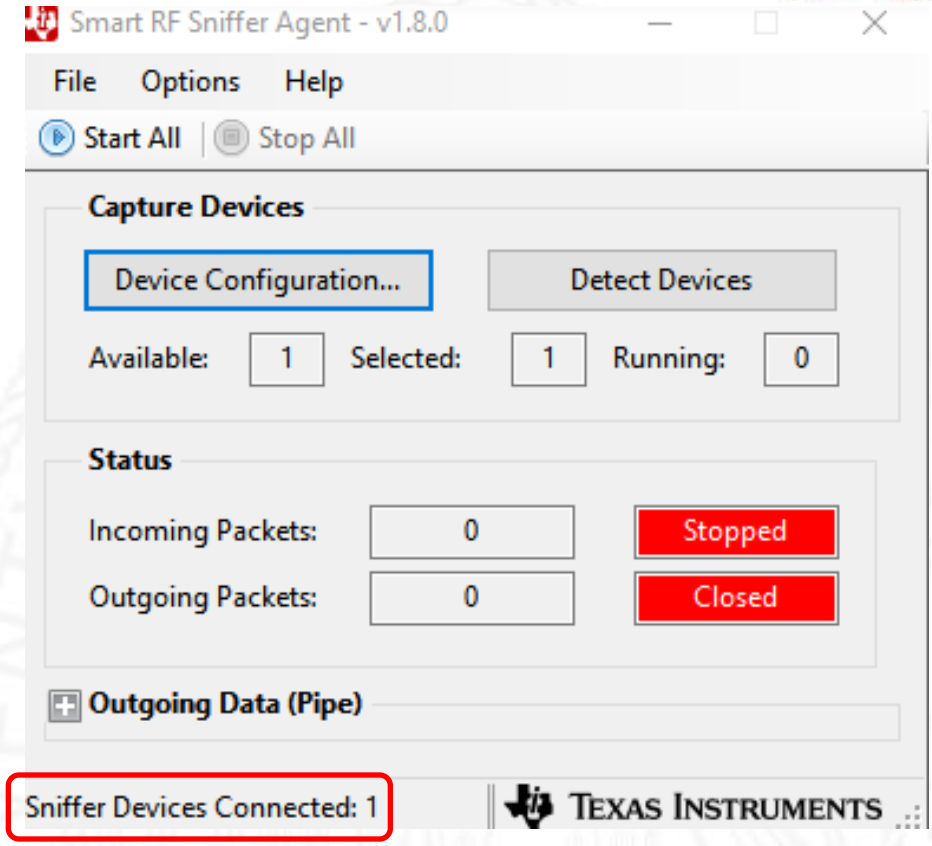

Figura 24. Smart RF Sniffer Agent con dispositivo sniffer detectado.[22]

La Figura 25 presenta el estado del dispositivo, su referencia, el puerto COM al que está conectado, el estado de operación (detenido) entre otros parámetros y es en esta ventana donde se tiene la posibilidad de alternar entre los distintos protocolos y frecuencias. Y en la Figura 26, se presenta el despliegue de la lista de protocolos admitidos en la que se encuentra el estándar IEEE 802.15.4 que corresponde a Zigbee

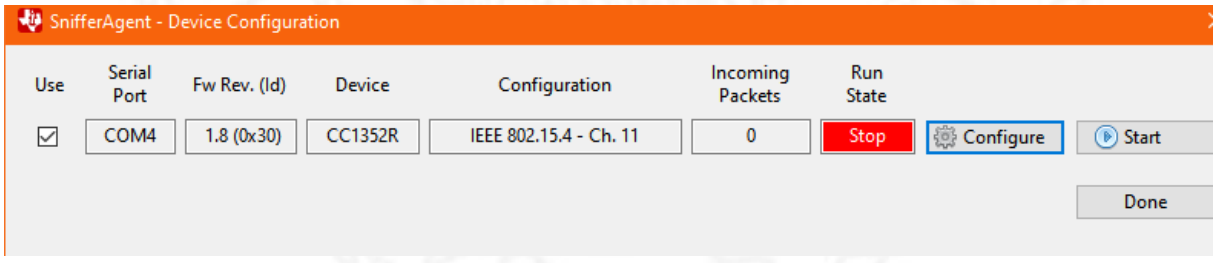

Figura 25. Configuración de dispositivo y visualización de estado de operación.[22]

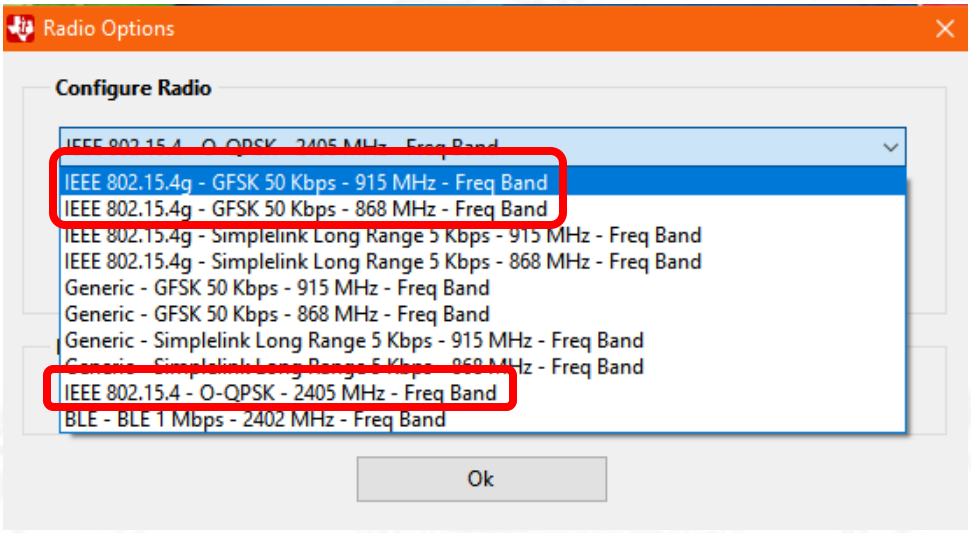

Figura 26. Selección de protocolos y frecuencias compatibles con el LaunchPad CC1352R.[22]

Una vez se ha realizado la configuración anterior y se ha seleccionado el protocolo que se dese entrar a capturar, el dispositivo ya está preparado para funcionar como Sniffer y es necesario solo vincularse con un Software visualización de tráfico como WireShark para empezar a capturar. En la Figura 27 el indicador de datos entrantes se vuelve verde y el indicador de datos salientes se vuelve azul. El icono del programa es azul.

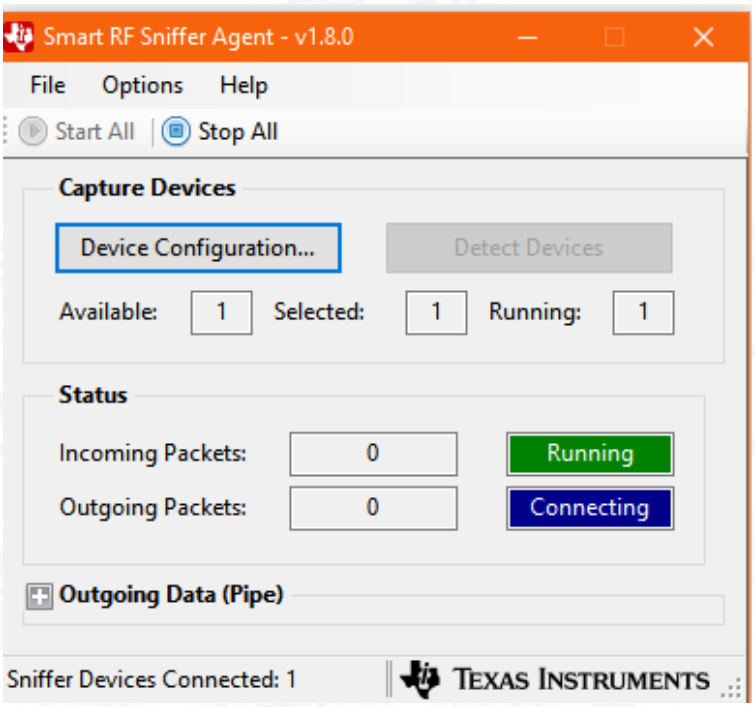

Figura 27. Smart RF con el LaunchPad funcionando planamente como Sniffer.[22]

9.3 Acondicionamiento de Wireshark.

Wireshark es un programa que permite ver el tráfico a través de las redes que está conectado sin embargo para poder utilizar este software es necesario tener las extensiones necesarias. Primero es necesario realizar un downgrade a la versión de Wireshark para contar con la versión 3.0.5 en la cual los propietarios de la tarjeta cuentan con unas extensiones compatibles., esto significa que tanto como el programa como las extensiones deben contar la misma versión, es necesario acceder al software de Wireshark como administrador para agregar dichas extensiones. En la Figura 28. Se encuentran resaltadas las tres extensiones para usar dispositivos de Texas instruments.

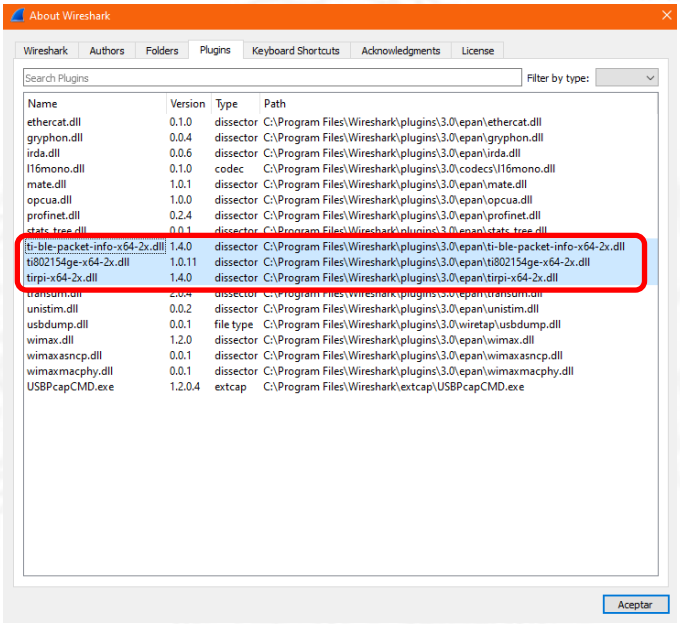

Figura 28. Extensiones de compatibilidad de hardware de Texas Instruments.[22]

Una vez habilitado la lectura de los protocolos Zigbee y dispositivos Texas instruments se realiza la creación del proyecto para el entorno que se desea analizar. Para esto es necesario ir al menú desplegable de Edit y a la sección de preferencias en donde se seleccionará en la columna de la izquierda el protocolo TI 802.15.4GE que hace referencia a Zigbee trabajando en hardware de Texas Instruments. Y lo siguiente, es añadir la Decryption Key por defecto que viene con los ejemplos de simplelink 15.4. $12:34:56:78:9A:BC:DE:F0:00:00:00:00:00:00:00:00$ como muestra la Figura 29. Esta key por defecto depende el fabricante del producto y varia del protocolo a utilizar.

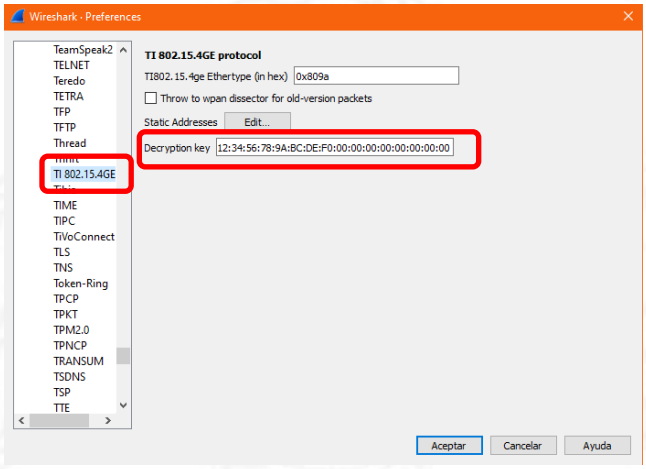

Figura 29. Selección de protocolo y asignación de decryption key.[22]

El software está preparado ahora para recibir paquetes en el protocolo 802.15.4, para que un equipo pueda ver los paquetes que transitan por la red es necesario tener los identificadores de EUI-64 y el identificador PAN los cuales sirven como contraseña para que nadie pueda ver lo que pase, con esto se permite acoplar un sniffer a una red sin romper ninguna regla de privacidad. Como se observa en la Figura 30.

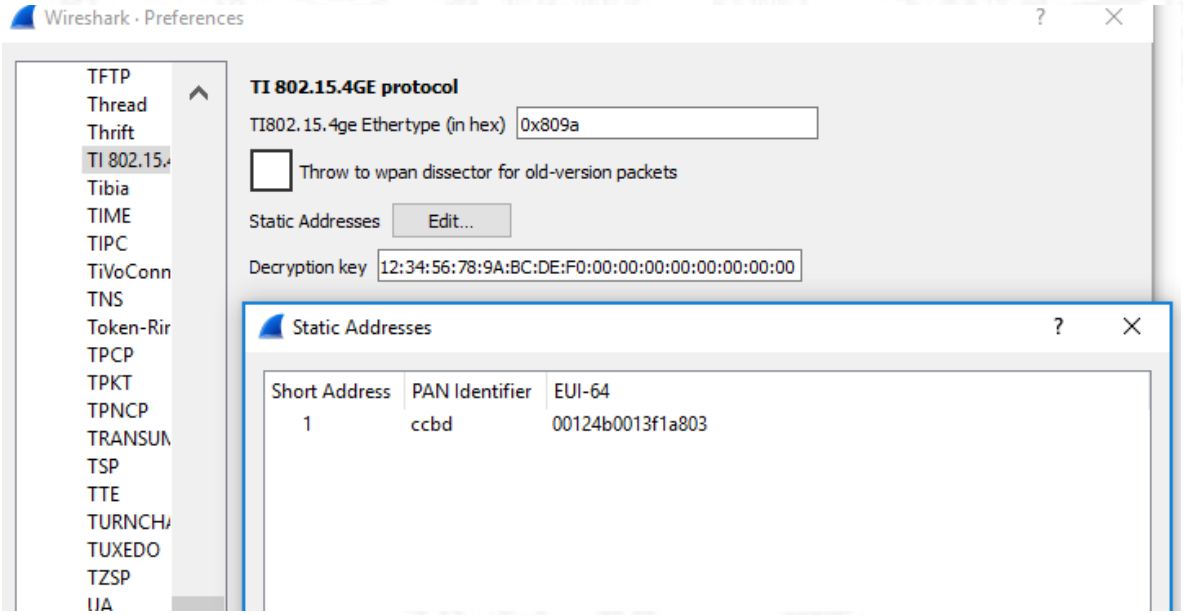

Figura 30. Introducción de PAN identifier y EUI-64.[22]

En la Figura 31 se observan los paquetes entrantes en Wireshark una vez se realizan los cambios en la configuración. Si todo quedo bien y se agregó bien los identificadores PAN se puede ver como Wireshark reconoce el protocolo con la sigla IEEE 802.15.4 diferenciado con color rojo, y en color verde se aprecia las tramas ZigBee con verde.

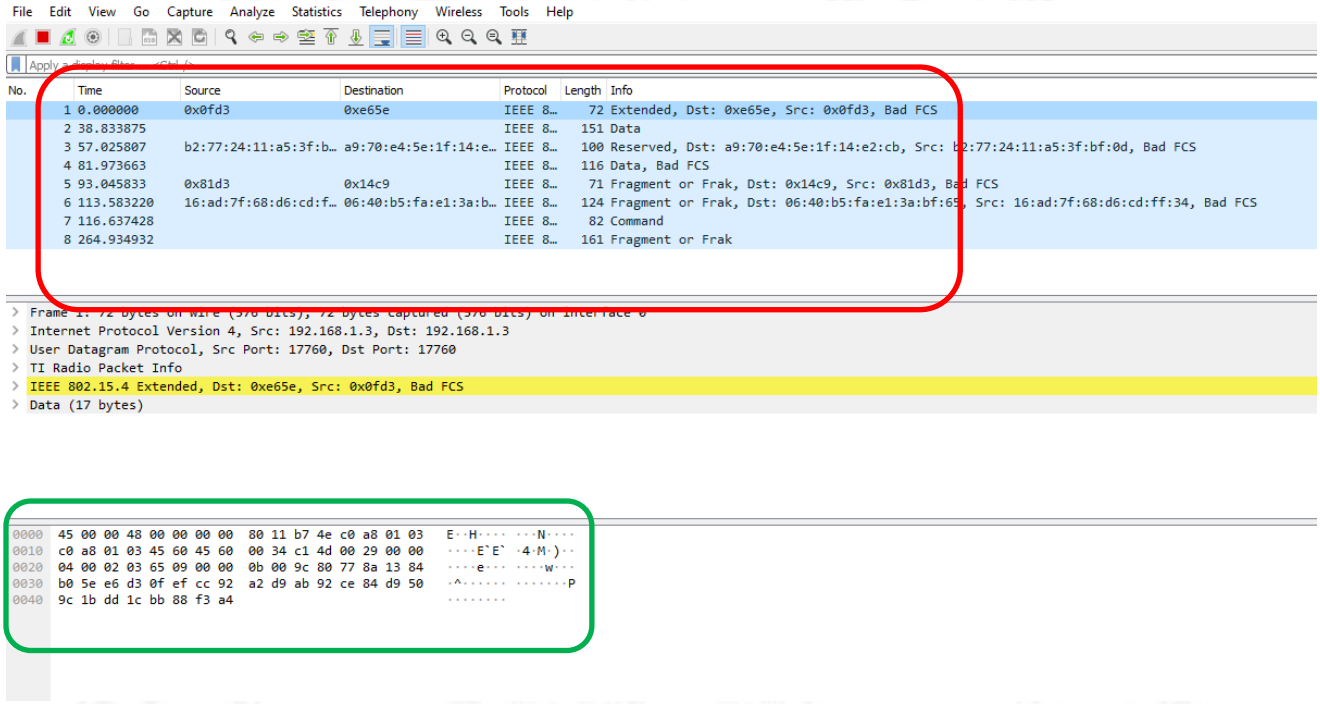

Figura 31. Paquetes recibidos por Wireshark en el protocolo 802.15.4.[22]

Wireshark ahora muestra los datos capturados y el ícono de Sniffer Agent se vuelve verde. Esto quiere decir que el toolbox está listo para empezar a recibir los paquetes de la red especificada.

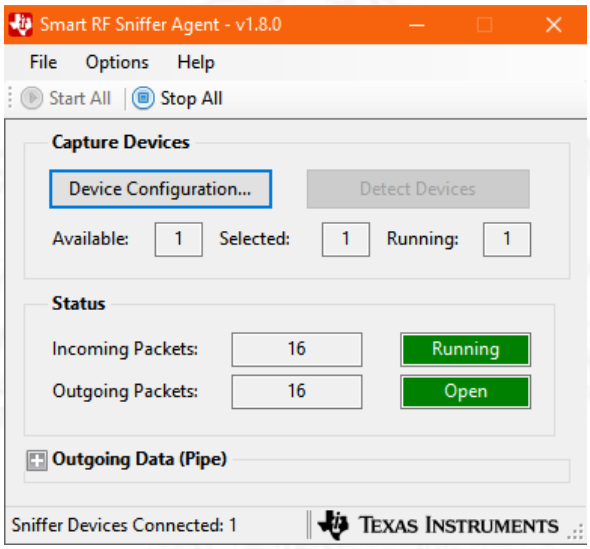

Figura 32. Interfaz de Smart RF Sniffer Agent con el LaunchPad CC1352R complemente funcional.[22]

El Sniffer Agent encapsula todos los paquetes en UDP / IP y los paquetes enviados al puerto UDP 17760 indican paquetes TI RPI (Radio Packet Info) como se observa en la Figura 32.

9.3.1 Hardware de sniffing

Como se ha descrito anteriormente un analizador de tráfico tiene un componente de software, pero también uno de hardware, que se encarga principalmente de “escuchar” la comunicación que se lleva a cabo en una red y en ocasiones también será capaz de almacenar la información escuchada.

Para que un hardware funcione como sniffing deberá cumplir con una serie de características, entre las principales se encuentran relacionadas con el protocolo que se desea capturar, ya que como es evidente el hardware debe ser capaz de comunicarse por dicho protocolo (para el caso de proyecto ATRAZ el protocolo a trabajar es Zigbee) y la otra característica más demandante será la frecuencia a la que opera el dispositivo.

El LaunchaPad CC1352R es una tarjeta que es distribuida por Texas Instruments y cumple con las características anteriormente expuestas, y también es un hardware que permite ser configurado para que pueda cumplir con las funciones de Sniffing. El Launchapad CC2531 cuenta con compatibilidad total con el Toolbox de Packet Sniffing. El hardware cuando se encuentra operable se ve de la forma en que aparece en la Figura 33.

Figura 33. Hardware capturador de tráfico en estado operativo y funcional.[22]

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

10 IMPLEMENTACION DEL PROYECTO ATRAZ.

Con el entorno de análisis de tráfico implementado, esta sección esta destina a mostrar cómo es el funcionamiento y desempeño en un escenario de la vida real. Debido a que la concepción de este proyecto está completamente involucrada con el proyecto PIICO y sus necesidades de saber cómo se desempeña el tráfico que circula por su red, a continuación, se describe como es el proceso de análisis de tráfico en la comunicación del nodo central y los remotos del proyecto PIICO en la universidad de San Buenaventura.

10.1 Entorno de análisis de trafico

Los datos obtenidos de Wireshark no son compatibles con entornos que sean diferentes a wireshark, por lo tanto, esta información debe ser procesada y adecuada para poder trabajar con ella en otros ambientes, esta sección presenta el proceso para migrar los datos de wireshark a otras plataformas como Matlab.

Para realizar un buen análisis del tráfico se deben tener en cuenta una serie de parámetros entre los cuales se encuentran el throughput y el retardo, en los cuales se enfocó el proyecto ATRAZ. Para poder reconocer estos parámetros se desarrolló una interfaz gráfica de usuario en Matlab que permitiera ver el graficado el throughput y se pudiera ver el retardo de cada paquete obtenido. A continuación, se describe también como fue construir este entorno gráfico.

Empleando la teoría del tele tráfico se encuentra que dichos parámetros están dados por las fórmulas:

$$D = L/R \qquad (1)$$

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

En donde D es el Retardo (delay en inglés), L hace referencia a la longitud del paquete (dato que se encuentra entre los que aporta Wireshark) y R es la tasa de transmisión del medio, la cual para Zigbee es de 250kbps.

$$Thoughput = MSS/T \qquad (2)$$

Para hallar el throughput es necesario tener también el tamaño del paquete denominado en la formula como MSS el cual esta proporcionado en la tabla de captura de Wireshark y es necesario dividir este valor por el valor del Tiempo para hallar el valor del throughput en cada instante de tiempo.

10.1.1 Interfaz gráfica de usuario

El software implementado para la creación de la interfaz gráfica de usuario fue Matlab, dado que es un sistema de cómputo numérico (Matemático) que posee un lenguaje de programación propio y que servirá a la hora de exportar los archivos csv separado por comas de wireshark, así mismo este software permite crear una aplicación ejecutable para que cualquier usuario que disponga de un computador de lo conseguido en este proyecto.

Una vez se ha generado un archivo con la captura de tráfico desde wireshark es necesario realizar una exportación de estos datos a un registro .csv separado por comas. Esto permite que se genere una tabla con solamente la información asociada a el número de paquetes, tiempo, destino, origen, protocolo, longitud del paquete e información de este capturado con wireshark. los datos de dicha tabla ahora son compatibles con Matlab. En la figura 34 se observa como desde la pestaña de File>Export Packet Dissections>As CSV se logra generar el archivo.

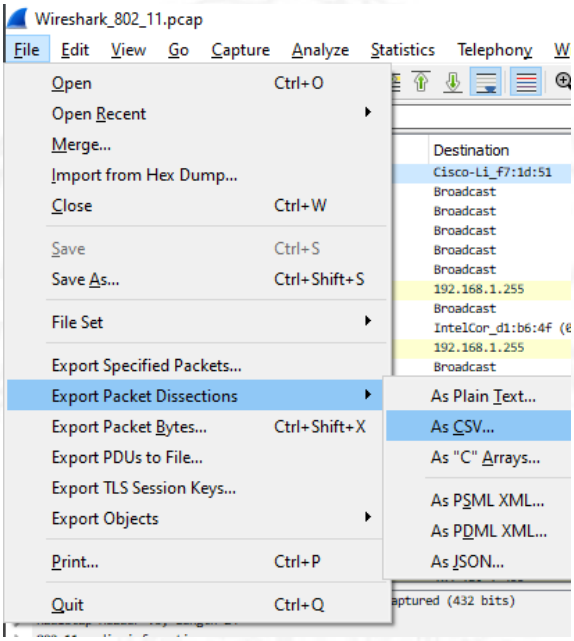

Figura 34. Exportación de paquetes obtenidos en wireshark a CSV [22]

Los archivos .CSV tienen la característica de guardar la información por filas y columnas, en la cual cada celda está dada por caracteres separados por comas esto se puede evidenciar en la Figura 35.

	A	B	C	D	E	F	G	H	I	J	K	L
1	No.,"Time","Source","Destination","Protocol","Length","Info"											
2	11,"553.657164","e5:fe:7a:d1:1d:ab:ef:90","82:ae:16:03:2c:1f:82:42","IEEE 802.15.4","138","Extended, Dst: 82:ae:16:03:2c:1f:82:42, Src: e5:fe:7a:d1:1d:ab:ef:90, Ba											
3	17,"780.595068","32:1c:4b:aa:38:6e:89:1e","10:e6:1a:56:8e:cf:25:4f","IEEE 802.15.4","154","Data, Dst: 10:e6:1a:56:8e:cf:25:4f, Src: 32:1c:4b:aa:38:6e:89:1e, Bad FCS											
4	19,"793.610617","0xc3a4","0xfb26","IEEE 802.15.4","117","Fragment or Frak, Dst: 0xfb26, Src: 0xc3a4, Bad FCS"											
5	21,"975.003563","ff:0c:46:44:3c:5b:82:fd","","IEEE 802.15.4","75","Reserved, Src: ff:0c:46:44:3c:5b:82:fd, Bad FCS"											
6	23,"1022.747858","18:35:0f:99:d1:5b:59:c8","94:c7:2d:c5:32:c0:8f:08","IEEE 802.15.4","137","Multipurpose, Dst: 94:c7:2d:c5:32:c0:8f:08, Src: 18:35:0f:99:d1:5b:59:c8											
7	25,"1144.074692","","","IEEE 802.15.4","104","Command, Bad FCS"											
8	27,"1166.751822","0xfeb9","5f:5c:28:1f:20:38:f8:30","IEEE 802.15.4","88","Reserved, Dst: 5f:5c:28:1f:20:38:f8:30, Src: 0xfeb9, Bad FCS"											
9	28,"1170.070392","0x02b9","","IEEE 802.15.4","149","Extended, Src: 0x02b9, Bad FCS"											
10	32,"1313.408704","de:6e:a3:0b:1d:e3:33:5a","0xd44b","IEEE 802.15.4","148","Ack, Dst: 0xd44b, Src: de:6e:a3:0b:1d:e3:33:5a, Bad FCS"											
11	33,"1352.330111","0x1d2c","85:f2:11:9a:bc:6b:f5:d5","IEEE 802.15.4","109","Extended, Dst: 85:f2:11:9a:bc:6b:f5:d5, Src: 0x1d2c, Bad FCS"											
12	61,"3309.790499","","","IEEE 802.15.4","146","Fragment or Frak, Bad FCS"											
13	73,"4081.905339","","62:e6:33:67:c1:ea:98:50","IEEE 802.15.4","120","Fragment or Frak, Dst: 62:e6:33:67:c1:ea:98:50, Bad FCS"											
14	83,"4465.395860","0x9bdd","e5:45:ae:ae:16:d0:8f:ea","IEEE 802.15.4","116","Fragment or Frak, Dst: e5:45:ae:ae:16:d0:8f:ea, Src: 0x9bdd, Bad FCS"											
15	88,"4653.609202","30:be:e9:a6:7c:cc:96:b3","61:de:f6:48:58:5a:dc:d5","IEEE 802.15.4","99","Fragment or Frak, Dst: 61:de:f6:48:58:5a:dc:d5, Src: 30:be:e9:a6:7c:cc:											
16	89,"4711.719232","","","IEEE 802.15.4","98","Enhanced Beacon, Bad FCS"											
17	91,"4714.718142","","da:f6:7b:ac:8f:38:cb:08","IEEE 802.15.4","162","Extended, Dst: da:f6:7b:ac:8f:38:cb:08, Bad FCS"											

Figura 35. Paquetes guardados en formato.CSV [22]

En cualquier interfaz de usuario se debe crear un background o borrador que almacenera posteriormente los datos como se observa en la figura 36, a la derecha se encuentra una tabla de celdas que aloja los datos .csv y que por medio de programación se logró obtener una interfaz que cumple con los requisitos para cumplir las necesidades del throughput y retardo; En el extremo superior izquierdo se encuentra un área para graficar que permite seleccionar mediante un menú desplegable se desean ver las métricas del rendimiento o el retardo. En la parte inferior de ella se encuentra la cantidad de Bytes que tiene el archivo y el análisis del Throughput, en la esquina superior derecha se encuentra una tabla conformada por la información .csv capturada por el sniffer de red capturada por wireshark y por último en la parte inferior derecha está el retardo de cada paquete que se puede manejar individualmente mediante una slider. Esto conforma la base de funcionamiento de la interfaz gráfica.

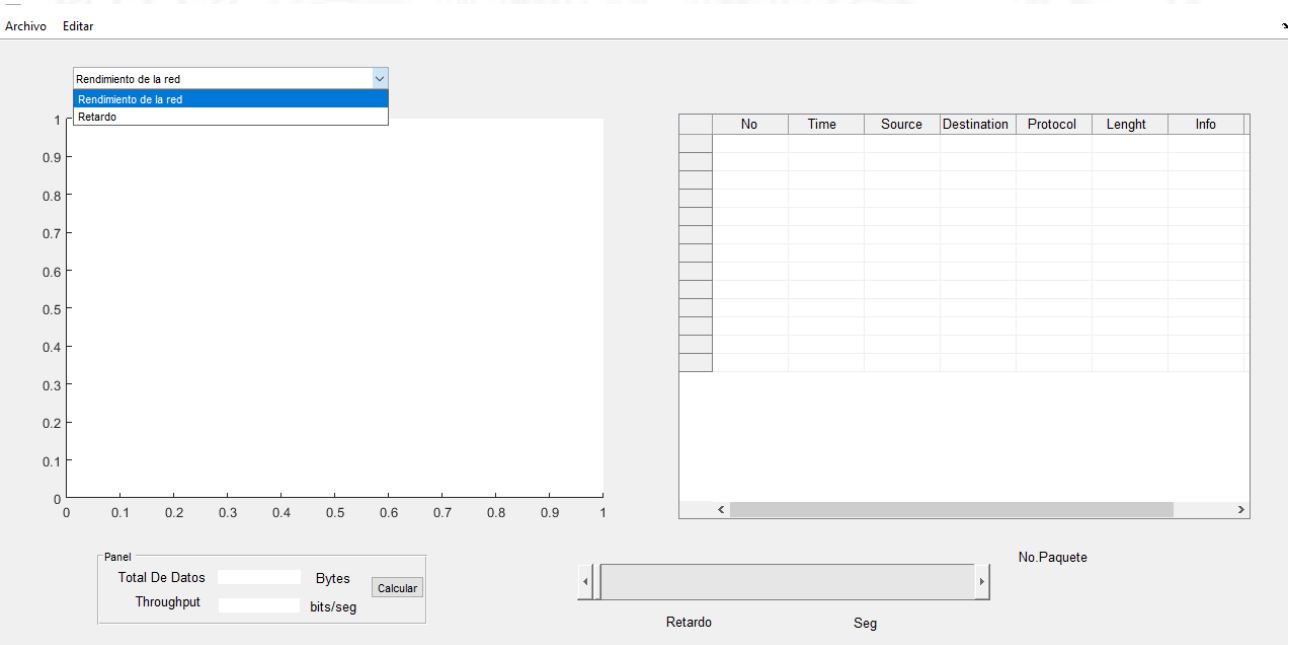

Figura 36. Base de la interfaz gráfica de usuario[22]

Para que la interfaz gráfica de usuario no estuviera limitada a funcionar con un solo archivo de datos capturados se procedió a crear un menú en el cual se cargan archivos

.xlsx (Excel) o .CSV, Este archivo .CSV es indispensable a la hora de unirlo ya que se debe convertir esta información en una tabla de Excel , para ello se importan los datos en Excel o CSV mediante el comando uigetfile de Matlab de la figura 37.

```
% --------------------------------------------------------------------
function ImportarTexto_Callback(hObject, eventdata, handles)

%Importar un archivo de texto o .csv
[nombre, direccion] = uigetfile({'*.csv', 'Archivo CSV'}, ...
                                'Escoge un archivo'); %Obtener nombre y dirección del archivo a importar
M = table2cell(readtable([direccion, nombre], 'ReadVariableNames', true));
NombresCol = M(1,:); %Separar el encabezado del arreglo y guardarlo como un arreglo nuevo.

NumeracionFilas = 0:size(M, 1);
set(handles.uitable1, 'Data', M, 'ColumnName', NombresCol, ...
    'ColumnEditable', logical(1:size(M,2)), 'RowName', NumeracionFilas);
guidata(hObject, handles);
```

Figura 37. Importación de archivo .CSV en Matlab[22]

Los datos obtenidos mediante el menú desplegable del GUI ahora son visibles mediante la tabla anteriormente creada de la figura 36.

El rendimiento de la red se aprecia mediante el grafico de los datos enviados (eje y) respecto al tiempo en segundos en que fue enviado (eje x) estos valores se obtienen de la tabla de tiempo y la longitud de los paquetes (Lenght) que posteriormente se grafican con el comando plot(x,y) en Matlab y se ejecuta una vez se presione en el botón de calcular, a continuación se puede apreciar en la figura 38.

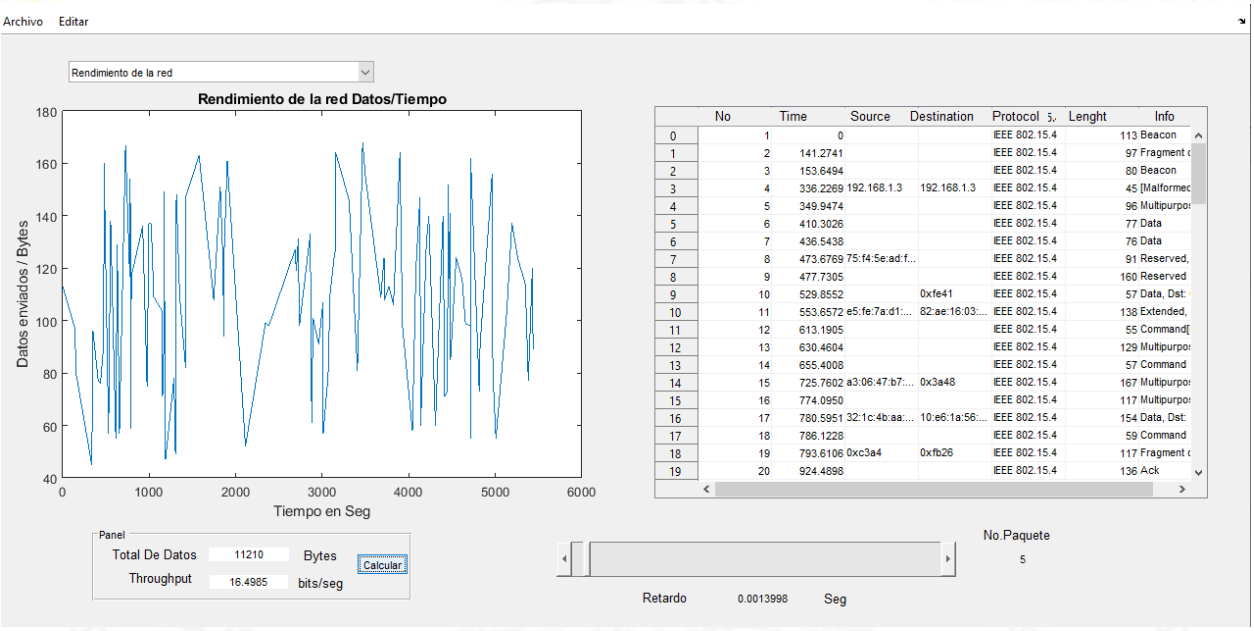

Figura 38. Ejemplo real siendo ejecutado por el GUI definitivo[22]

El ejemplo de la Figura 38 corresponde a las métricas del proyecto PIICO que se tomaron en los Laboratorios de la Universidad y son la base para el análisis de la red Zigbee.

Si se realiza una suma de todos los paquetes se puede obtener el total de los datos, en el panel inferior a la izquierda se puede distinguir que para la figura 38 fueron de 11210 bytes u 11.210Mb esta sumatoria se realiza mediante el comando sum(cell2mat(T(:,6))) que permite realizar la suma que existe en la celda de la tabla creada que va desde 0 hasta todos los datos que posee y que se limita por la columna 6 , en este caso es la columna Lenght a la cual se le asocia los datos enviados.

Además de lo anterior, es necesario tener en cuenta que el throughput es un elemento importante a la hora de evaluar cualquier red ya que permite conocer la velocidad a la cual fluye la información en un sistema, este dato corresponde a la ecuación de la ecuación (2). La Figura 39 permite ver como en Matlab se puede hacer de forma ágil y

rápida el cálculo mediante sumatorias y divisiones con los datos suministrados por la tabla.

```
[m,n] = size(T)
handles.sumatorial = sum(cell2mat(T(:,6))); %% columna 6  // suma de la columna
handles.sumatoria2  = cell2mat(T(m,2)); %% columna 2  //ultimo valor de la fila
handles.sumatoria3  = (cell2mat(T(:,6)));
handles.sumatoria4  = (cell2mat(T(:,2)));

numerador= [handles.sumatorial]
denominador=[handles.sumatoria2]

% final=str2num(numerador)/str2num(denominador)
handles.throuhgput=((numerador)./(denominador))*8 %% divido en 8 bits

set(handles.sumal, 'String', num2str(handles.sumatorial ));
set(handles.suma2, 'String', num2str(handles.throuhgput));

x=handles.sumatoria4;%%tiempo
y=handles.sumatoria3;%%longitud

handles.sumatoria5  = cell2mat(T(bl,2)) %%retardo
```

Figura 39. Datos que conforman el Thoughput del GUI.[22]

La topología, la demanda de paquetes y el ancho de banda son características diferentes para cada red y por tanto varía dependiendo según las necesidades del sistema, sin embargo, se busca que el QoE (Quality Of Experiencie) sea lo mejor posible, entre más alto sea el Thoughput mejor será el desempeño de la transmisión, midiéndose en bites por segundo.

10.1.2 Análisis de la Interfaz gráfica de usurario

Una interfaz de usuario desde su principio radica en la interacción entre elementos del del sistema con un elemento externo o usuario, por lo tanto la interfaz debe ser amigable con este último, esta amigabilidad se refiere a la facilidad con el que el usuario manipula la interfaz, que así mismo debe relacionarse con la interactividad que tiene con el usuario, debe ser comunicativo, presentarle de manera clara y fácil al usuario una idea que transmitir, bien sea de manera visual, textual o con símbolos.

Una vez la interfaz cumpla con estos requisitos mínimos, debe responder a las necesidades por la cual fue diseñada, con el fin de que tenga éxito.

El GUI de ATRAZ busca en primera medida que cualquier persona sin un conocimiento previo de redes pueda manipular la interfaz sin ningún problema,(exportar y cargar archivos), como se implementa en la Figura 38, allí en la parte superior se puede apreciar un menú desplegable Archivo>Exportar con el cual solo se debe cargar datos previamente obtenidos, una vez se realiza la acción se procede a calcular el rendimiento de la red mediante el botón de calcular, esta manera clara(visual) por medio de gráficos permite que una persona asocie la gráfica con la gráfica de rendimiento de un CPU, el rendimiento de una red Zigbee en general se basa en su topología, tipos de tráfico y arquitectura que la persona desee implementar de acuerdo a sus necesidades, esto se aborda más en detalle en el capítulo 7.2, 7.3 y 7.31. Por lo tanto el rendimiento de una red se fundamenta independientemente de sus características por medio de su retardo y velocidad de transferencia final, estas características son principales a la hora de evaluar una red dado que se puede tener una estimación de cuanto tarda en llegar un paquete de un lugar a otro, o cuanto se demoró en enviarlo, este simple análisis de retardo en paquetes logra predecir si una red envía los paquetes de manera ágil y rápida o por el contrario lento e ineficaz, si el retardo es demasiado lento se puede abstraer que la red en la cual está diseñada debe tener un cambio bien sea en su topología, arquitectura o rango, esta última es la más fácil de variar y validar los cambios, debido a que busca la línea de vista; entre el receptor y emisor mediante una corta distancia.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

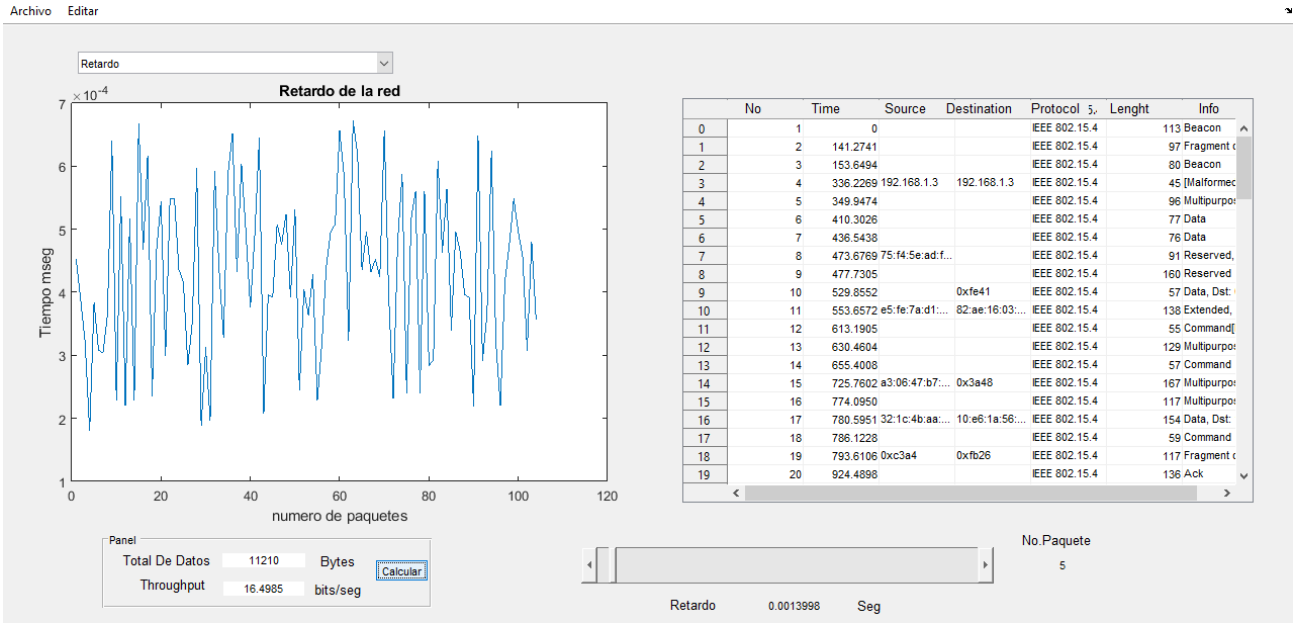

Figura 40. Métrica del retardo en el GUI.[22]

La Figura 40 permite ver en detalle el retardo de la red donde se aprecia el eje(y) el tiempo que le tomo llegar al paquete de acuerdo a la ecuación(1) y en el eje(x) está el número del paquete que se analizó, este retardo se puede ver individualmente con el slider al costado inferior derecho del GUI como se muestra en la misma Figura, la gráfica permite apreciar las unidades del tiempo en milis segundos por lo cual se logra ver que el retado para la red de PIICO está entre los 0.2 mili Seg y 0.7 mil Seg, es un tiempo bastante corto en el que el transmisor coloca los bits en el canal, este tiempo siempre se busca que este sea el más bajo. La red de PIICO es estable debido a que no se encuentran anomalías en sus retardos o grandes cambios de unidades.

En cuanto al throughput es una unidad unidimensional que busca darle un valor a la red con el cual se pueda medir, esta medida se toma en bits por segundo, inicialmente es importante revisar las unidades de medida que proyecta wireshark, debido a que la longitud de paquetes está en Bytes es necesario hacer una conversión de unidades, el proceso para pasar de Bytes(B) a Bits por segundo(bps) se realiza multiplicando los

Bytes por 8, esto se debe a que un 1 Byte equivale a 8 Bits en la Figura 39 se aprecia como se relacionan los conceptos anteriores en Matlab.

El valor arrojado permite calcular la utilización de dicho enlace que necesita la red para transferir de manera correcta los paquetes. Este dato se observa nuevamente en la Figura 38 en la parte inferior izquierda y se aprecia que El throughput para la red de PIICO de ejemplo es de 16,49 bits/seg. El valor obtenido es bastante acorde a la tasa de transmisión de Zigbee 250Kbps a 2,4Ghz, y permite inferir que la red se encuentra muy bien balanceada[3] por lo cual no es necesario mover, cambiar la topología o estructura interna, debido a que los datos enviados no tienen una demanda alta de paquetes.

11 DISCUSIÓN

Para lograr Identificar los componentes necesarios para la construcción de un analizador de tráfico para redes Zigbee, se realizó una amplia investigación en la que se detalla que es un analizador de tráfico, en que consiste, que elementos lo componen y con qué componentes podrían abastecer las necesidades para la construcción de uno para el protocolo Zigbee.

De lo anterior, se obtuvo que un analizador de tráfico constaba de un componente de hardware cuyo propósito es el de captar el flujo que circula por una red y, su integración con un componente de software que se encarga de realizar una interpretación para visualizarlos claramente y que los datos capturados se conviertan en información útil para el usuario.

[3] Una red balanceada se asocia a que su retardo es muy bajo y su throughput está por debajo de la tasa de transmisión.

Con respecto al hardware, es necesario que cumpla una serie de características para garantizar la compatibilidad total; estas particularidades pueden verse reducidas a tres y se considera que deben ser las siguientes: Ser configurable, debe poder comunicarse con el protocolo Zigbee (para el caso específico de este proyecto) y finalmente, trabajar en las frecuencias que se desean analizar.

Se realizó una búsqueda de un dispositivo que cumpliera estas características y que además se encontrara dentro del presupuesto aprobado, por esto se realizaron comparativas entre distintos dispositivos y dada su compatibilidad con un Toolbox de análisis de tráfico, su accesible precio, mejor desempeño y mejores prestaciones, se optó por utilizar el LaunchPad de Texas Instruments de referencia CC1352R como dispositivo de captura de tráfico, trabajando en conjunto a la aplicación Smart RF Packet Sniffing también de Texas Instruments.

En cuanto a la ejecución de los objetivos dos y tres, el progreso de los mismo a mitad de desarrollo se vio truncado, debido a las circunstancias relacionadas con la pandemia mundial.

Finalmente, dentro del software a trabajar se estableció WireShark como interfaz de usuario debido a que cuenta con compatibilidad con los equipos utilizados a lo largo del desarrollo del analizador de tráfico. De esta manera se da finalmente una solución para cumplir las necesidades de sistemas con características similares a PIICO en cuanto a análisis capturado, visualizado en una plataforma matemático para el análisis del tráfico que sirve para implementarlo no solo en el proyecto PIICO con el que originalmente se planteó dar solución sino que puede ser implementado en otras red Zigbee, así mismo los dispositivos que cumplieron las características fueron pensados para las futuras investigaciones que desean explorar más el campo del tráfico Zigbee al ser dispositivos con más recursos para expandir el conocimiento del protocolo IEEE 802.15.4.

Es de resaltar que la investigación se finiquitó acorde a las fechas, objetivos y que está relacionada con las topologías del protocolo, las tramas que se manejan, la seguridad de este, construcción de una red Zigbee, construcción de la interfaz gráfica de usuario.

12 CONCLUSIONES

El proyecto ATRAZ ha encontrado una solución alternativa a hardware existentes que se disponen para la captura del tráfico del protocolo Zigbee. En el mercado los hardware desarrollados alcanzan precios muy altos y aun así cuentan con grandes limitaciones relacionadas a la frecuencia, No obstante, gracias a la solución de hardware implementada en el proyecto ATRAZ es posible explorar las bandas de 2.4 GHz y también bandas de frecuencia Sub-1GHz (Las bandas de 895 MHz y 915 MHZ), lo que lo vuelve un analizador completo en cuanto a Zigbee se refiere.

Con la configuración realizada al LaunchPad CC1352R fue posible que un dispositivo que, en condiciones normales es un sistema embebido cuya función principal no se centra en la captura de tráfico, se adapte para que pueda realizar esta tarea y permitiera observar las tramas del protocolo Zigbee con ayuda del software Smart RF Packet Sniffer de Texas instruments.

Con la solución implementada en el proyecto ATRAZ, el proyecto PIICO puede satisfacer las necesidades de análisis de tráfico y con lo cual es posible realizar una valoración de la comunicación entre los nodos y determinar la eficiencia de la red mediante los parámetros del retardo y el throughput entregados por el sistema.

La métrica del throughput o rendimiento, corresponde a un parámetro que es complicado de valorar en cualquier área, no solo en las telecomunicaciones, esto debido a que características que varían d una red a otra como lo son las topologías utilizadas, la demanda de paquetes, el ancho de banda dispuesto y la cantidad de dispositivos, hacen

que las necesidades para cada Red sean también diferentes y no se le exija lo mismo a este tipo de redes.

Las pruebas realizadas en el proyecto PIICO permiten identificar tramos en los que la señal no es perfectamente regular, al ser una red que envía datos periódicamente, no debería ocurrir, sin embargo, gracias al análisis de tráfico realizado es posible identificar que si bien no es una pérdida de información dañina si es posible solucionarla adoptando un envío de paquetes redundante para garantizar el envió del 100% de la información.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

13 INFORME DE PRESUPUESTO EJECUTADO

Rubros Aprobados	Monto Aprobado	Monto Ejecutado	Detalle de Gastos
Equipos	$500.000	$304.000	Sistema de comunicación inalámbrico **Suministro 8498.** Compra internacional, material entregado el 19 de noviembre. Se aclara que este ítem tenía una reserva de $90.000 para impuestos. Finalmente, no se causaron estos costos por parte de la DIAN.
Total de Gastos	$500.000.	$304.000	Se tiene una ejecución del 60 %. Se aclara que se tenían planeado la compra de otros dispositivos necesarios para implementar los escenarios de prueba de la red zigbee, el monto ascendía a $164.000, pero no se podía generar la solicitud de compra hasta que no se conociera el monto final disponible después de impuestos del suministro 8498.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

14 Anexos

Los resultados obtenidos se encuentran a continuación en la Tabla 5. La cual se organiza con los Objetivos a la izquierda seguido de los resultados que se obtuvieron, el producto que salió de este resultado y el estado en el que se encuentra, finalmente está el nombre con el cual se culminó el objetivo.

Tabla 5. Resultados del proyecto y estado de avance.

Objetivos	Resultados	Productos	Estado de avance	Nombre
Identificar los componentes necesarios para la construcción de un analizador de tráfico para redes Zigbee.	Tablas de comparativa de dispositivos y software para análisis de tráfico Zigbee	Informe Final de investigación	100%	8° Encuentro Institucional y 7° Distrital de Semilleros de Investigación - Universidad Minuto de Dios. Se anexan certificados de participación de los semilleristas.
	Ponencia en evento científico (Este producto no estaba comprometido debido a las condiciones de la pandemia)	Ponencia en encuentro de semilleros de la Universidad Minuto de Dios		
Desarrollar el analizador de tráfico y la programación de la aplicación software que permita la generación de las métricas necesarias para determinar el rendimiento de la red.	Red Zigbee como entorno investigativo y de análisis	Informe Final de investigación	100 %	Informe final de investigación.
	Hardware adaptado para capturar tramas del protocolo Zigbee	GC. Generación de contenido	100 %	Informe final de investigación.
	Integración de hardware y software funcional para captura de tráfico Zigbee			

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

Evaluar la herramienta desarrollada mediante la captura y análisis de tráfico ZigBee.	Set de pruebas llevadas a cabo para evaluar el desempeño del sistema de análisis de trafico	GC. Generación de contenido	100%	Informe final de investigación.

Además de lo anterior se anexan el código en Matlab (anexo 1), los certificados de ponencia (anexo 2) y el Video explicativo (anexo 3) Con el siguiente link de acceso;

https://teams.microsoft.com/_#/school/files/General?threadId=19%3Acd87e7887576439fb1f3f35795dffb15%40thread.tacv2&ctx=channel&context=Anexos&rootfolder=%252Fsites%252FAnteproyectodeGrado6977%252FShared%2520Documents%252FGeneral%252FAnalizador%2520de%2520Tr%25C3%25A1fico%2520Zigbee_ATRAZ%252FAnexos

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

15 BIBLIOGRAFÍA.

[1] M. Ruiz, E. Álvarez, A. Serrano, and E. Garcia, “The Convergence between Wireless Sensor Networks and the Internet of Things; Challenges and Perspectives: a Survey,” *IEEE Lat. Am. Trans.*, vol. 14, no. 10, pp. 4249–4254, Oct. 2016, doi: 10.1109/TLA.2016.7786301.

[2] M. C. Vega, P. O. Vivas, C. M. Rios, C. G. Luis, B. C. Mart\’\in, and A. H. Seco, *Las tecnolog{\’\i}as IOT dentro de la industria conectada: Internet of things*. Fundación EOI, 2015.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[4] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols: Review,” in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690, doi: 10.1109/ICITECH.2017.8079928.

[5] W. Li and C. Chou, “Design and Implementation of a Zigbee-based Communication Substrate for Wireless Sensor Networks µL½u · P ´ úºô ¸ ¤§ Zigbee ³q ° T ¥ - x^ao3] -p » P¹ê § @.”

[6] J. W. Chong, H. Y. Hwang, C. Y. Jung, and D. K. Sung, “Analysis of throughput and energy consumption in a ZigBee network under the presence of bluetooth interference,” *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 4749–4753, 2007, doi: 10.1109/GLOCOM.2007.901.

[7] A. Sikora and V. F. Groza, “Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band,” in *2005 IEEE Instrumentationand Measurement Technology Conference Proceedings*, vol. 3, pp. 1786–1791, doi: 10.1109/IMTC.2005.1604479.

[8] R. G. Garroppo, L. Gazzarrini, S. Giordano, and L. Tavanti, “Experimental

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices," in *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Jun. 2011, pp. 1–9, doi: 10.1109/WoWMoM.2011.5986182.

[9] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Co-existence of Zigbee and WLAN, A Performance Study," in *2006 Wireless Telecommunications Symposium*, Apr. 2006, pp. 1–6, doi: 10.1109/WTS.2006.334532.

[10] I. Howitt and J. A. Gutierrez, "IEEE 802.15.4 low rate - wireless personal area network coexistence issues," in *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.*, vol. 3, pp. 1481–1486, doi: 10.1109/WCNC.2003.1200605.

[11] M. Kang, J. Chong, H. Hyun, S. Kim, B. Jung, and D. Sung, "Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference," in *2007 2nd International Symposium on Wireless Pervasive Computing*, 2007, doi: 10.1109/ISWPC.2007.342601.

[12] B. Jung *et al.*, "Ubiquitous Wearable Computer (UWC)-Aided Coexistence Algorithm in an Overlaid Network Environment of WLAN and ZigBee Networks," in *2007 2nd International Symposium on Wireless Pervasive Computing*, 2007, doi: 10.1109/ISWPC.2007.342603.

[13] M. Xu, L. Ma, F. Xia, T. Yuan, J. Qian, and M. Shao, "Design and implementation of a wireless sensor network for smart homes," *Proc. - Symp. Work. Ubiquitous, Auton. Trust. Comput. Conjunction with UIC 2010 ATC 2010 Conf. UIC-ATC 2010*, vol. 2, no. 2, pp. 239–243, 2010, doi: 10.1109/UIC-ATC.2010.16.

[14] J. W. Chong, H. Y. Hwang, C. Y. Jung, and D. K. Sung, "Analysis of Throughput and Energy Consumption in a ZigBee Network Under the Presence of Bluetooth Interference," in *IEEE GLOBECOM 2007-2007 IEEE Global Telecommunications Conference*, Nov. 2007, pp. 4749–4753, doi: 10.1109/GLOCOM.2007.901.

[15] D. Dobrilovic, Z. Stojanov, V. Brtka, Z. Covic, and N. Bilinac, "Software application for analyzing ZigBee network performance in university courses," *SISY 2014 - IEEE 12th Int. Symp. Intell. Syst. Informatics, Proc.*, pp. 73–77, 2014, doi:

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

10.1109/SISY.2014.6923560.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[17] J. Luo, “A ZigBee and Sip-Based Smart Home System Design and Implementation,” *Int. J. Online Eng.*, vol. 13, no. 1, pp. 42–60, 2017, doi: 10.3991/ijoe.v13i01.6258.

[18] Texas Instruments, “SmartRF ™ Packet Sniffer User Manual,” vol. swru187f, p. 31, 2011.

[19] E. D. Ngangue Ndih and S. Cherkaoui, “On Enhancing Technology Coexistence in the IoT Era: ZigBee and 802.11 Case,” *IEEE Access*, vol. 4, pp. 1835–1844, 2016, doi: 10.1109/ACCESS.2016.2553150.

[20] G. V Vivek and M. P. Sunil, “Enabling IOT services using WIFI - ZigBee gateway for a home automation system,” in *2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Nov. 2015, pp. 77–80, doi: 10.1109/ICRCICN.2015.7434213.

[21] Firdaus, E. Nugroho, and A. Sahroni, “ZigBee and wifi network interface on Wireless Sensor Networks,” *Proceeding - 2014 Makassar Int. Conf. Electr. Eng. Informatics, MICEEI 2014*, no. March, pp. 54–58, 2014, doi: 10.1109/MICEEI.2014.7067310.

[22] W. yardane villamil Leandro Sanchez, “No Title.” Bogota,DC, 2021.

[23] M. S. Hansen, “ZigBee Medical Sensor Networks,” *Coexistence*, no. June, 2006.

[24] “zigbee.” [Online]. Available: ftp://ftp1.digi.com/support/documentation/html/manuals/ZigBee/Introduction/zigbee.htm.

[25] Drew Gislason, Ed., “Commissioning ZigBee Networks,” in *Zigbee Wireless Networking*, Elsevier, 2008, pp. 331–350.

[26] D. De, R. Inalámbrica, M. A. Dávila, J. F. Pérez, W. Mantilla, and J. E. Moreno,

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia

"Diseño de una red inalámbrica tipo ZigBee para la implementación de un sistema domótico," no. November 2016, 2017, [Online]. Available: https://www.researchgate.net/publication/311207799_Diseno_de_una_red_inalambrica_tipo_ZigBee_para_la_implementacion_de_un_sistema_domotico.

[27] Jorge Pablo Dignani, "Trabajo final integrador de especialización en Redes y Seguridad," p. 42, 2011, doi: 10.1007/s11367-008-0053-5.

[28] L. Tian, M. Li, Z. Chen, and B. Guan, "Design of Smart Home Control Terminal Based on ZigBee and Electronic Technology," 2012, pp. 339–344.

[29] L. Yang, M. Ji, Z. Gao, W. Zhang, and T. Guo, "Design of Home Automation System Based on ZigBee Wireless Sensor Network," in *2009 First International Conference on Information Science and Engineering*, 2009, pp. 2610–2613, doi: 10.1109/ICISE.2009.481.

[30] M. Barrera Durango, N. Londoño Ospina, J. Carvajal, and A. Fonseca, "Análisis y diseño de un prototipo de sistema domótico de bajo costo," *Rev. Fac. Ing.*, no. 63, pp. 117–128, 2012.

[31] U. Guide, "XBee®/XBee-PRO S2C Zigbee®."

[32] M. Gamba, A. Gonella, and C. E. Palazzi, "Design issues and solutions in a modern home automation system," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2015, pp. 1111–1115, doi: 10.1109/ICCNC.2015.7069505.

[33] C. A. Vera Romero, J. E. Barbosa Jaimes, and D. C. Pabón González, "Configuration Parameters in Module XBEE-PRO® ZB S2B for Measuring Environmental Variables," *Tecnura*, vol. 19, no. 45, pp. 141–157, 2015, doi: 10.14483/udistrital.jour.tecnura.2015.3.a11.

[34] M. Loyola and P. Becerra, "Manual para la aplicación de la Tecnología Zigbee para edificios Inteligentes," pp. 5–7, 2015, [Online]. Available: https://dspace.ups.edu.ec/bitstream/123456789/7986/1/UPS-CT004855.pdf.

[35] J. Montesino, "UNIVERSIDAD POLITÉCNICA DE CARTAGENA Proyecto Fin de Carrera Red de sensores auto-configurable mediante tecnologías ZigBee y Arduino

con monitorización por aplicación Android," 2013.

[36] A. Oyarce, P. Aguayo, and E. Martin, "Guía del usuario Xee series 1," *… . olimex. cl/pdf/Wireless/ZigBee/XBee …*, pp. 1–69, 2010, [Online]. Available: http://www.hmangas.com/Electronica/Datasheets/Shield XBee Arduino/XBee-Guia_Usuario.pdf.

[37] 3Cu Electrónica, "comandos at 1." https://sites.google.com/site/3cuelectronica/home/comandos-at-1.

[38] Texas Instruments, "CC2531 USB Dongle Reference Design," 2021. https://www.ti.com/tool/CC2531USB-RD.

[39] Texas Instruments, "LAUNCHXL-CC1352R1," 2021. https://www.ti.com/store/ti/en/p/product/?p=LAUNCHXL-CC1352R1.

[40] D. Key, "Módulos de radio frecuencia (RF) Digi XBee® S1 802.15.4," 2021. https://www.digikey.com/es/product-highlight/d/digi-intl/digi-xbee-s1-802-15-4-rf-modules.

[41] Suconel, "Antena Sma Hembra De 900Mhz ANT900," *2021*, 2021. https://suconel.com/product/antena-sma-hembra-de-900mhz/.

[42] A. A. S. Martin *et al.*, "Análisis funcional para la Plataforma IoT PIICO," Universidad de san buenaventura, 2020.

[43] Texas Instruments, "LPSTK-CC1352R," 2021. https://www.ti.com/tool/LPSTK-CC1352R.

[44] K. N. X. Rf, "CC1352R SimpleLink ™ High-Performance Multi-Band Wireless MCU," no. February, 2020.

Carrera 8 H n.° 172-20 • PBX: 667 1090
Línea gratuita nacional: 01 8000 125151
www.usbbog.edu.co • Bogotá, D. C. - Colombia