UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Análisis y evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P

AUTORA:
Cabezas Chalco, Gloria Piedad

Trabajo de Titulación previo a la obtención del título de
INGENIERO EN TELECOMUNICACIONES

TUTOR:
Bohórquez Escobar, Celso Bayardo

Guayaquil, Ecuador

15 de Septiembre del 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Sra. **Cabezas Chalco, Gloria Piedad** como requerimiento para la obtención del título de **INGENIERA EN TELECOMUNICACIONES**.

TUTOR

_____

Bohórquez Escobar, Celso Bayardo

DIRECTOR DE CARRERA

_____

Heras Sánchez, Miguel Armando

Guayaquil, a los 15 del mes de Septiembre del año 2017

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Cabezas Chalco, Gloria Piedad**

DECLARÓ QUE:

El trabajo de titulación **"Análisis y evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P"** previo a la obtención del Título de **Ingeniera en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 15 del mes de Septiembre del año 2017

EL AUTOR

_____

CABEZAS CHALCO, GLORIA PIEDAD

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Cabezas Chalco, Gloria Piedad**

Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Análisis y evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

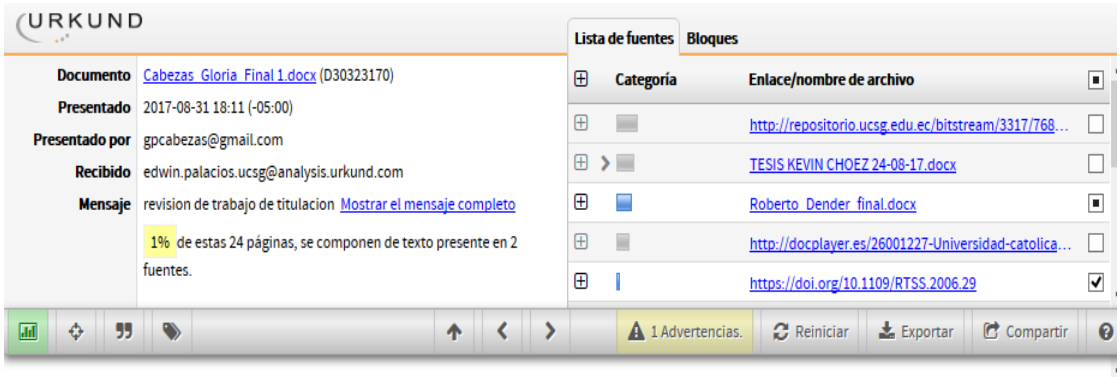
Guayaquil, a los 15 del mes de Septiembre del año 2017

EL AUTOR

_____

CABEZAS CHALCO, GLORIA PIEDAD

REPORTE DE URKUND



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Análisis y

evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P

AUTORA: Cabezas Chalco, Gloria Piedad

Trabajo de Titulación previo a la obtención del grado de INGENIERO EN TELECOMUNICACIONES

TUTOR: Bohórquez Escobar, Celso Bayardo

Guayaquil, Ecuador

DEDICATORIA

Este logro a mi Dios todo poderoso por estar siempre a mi lado y nunca abandonarme en los momentos más difíciles de mi vida, gracias por permitirme llegar hasta aquí, y ser una INGENIERÍA EN TELECOMUNICACIONES derramando sobre mi amor, bendiciones, éxitos y enseñanzas, sin ti no hubiese sido posible esté propósito.

A mis padres, quienes me han cuidado, protegido, inculcado valores y darme la confianza para alcanzar el objetivo de ser INGENIERA EN TELECOMUNICACIONES.

A mis tres hijos, Carlita, Lenin y Gabriel les dedico todos mis logros para que se sienta orgullosa de su mami y ayudarlos todos los días de mi vida.

A Stalin Cajas por darme su amor incondicional, ser maravilloso, apoyándome y acompañándome en todas las actividades de mi carrera, gracias por soportarme durante mi formación académica.

LA AUTORA

CABEZAS CHALCO, GLORIA PIEDAD

AGRADECIMIENTO

A Dios por guiarme por el buen camino, por darme salud y paz, llenándome de mucha sabiduría y entendimiento.

A mis padres e hijos por ser mis pilares fundamentales en mi vida y en mi formación académica, ayudándome en todo lo que necesite y teniendo siempre su apoyo condicional, en los buenos y no tan buenos momentos para culminar con éxito la carrera de Telecomunicaciones, los quiero mucho.

A mi hermana Martha y su esposo Omar porque sé que cuento con ellos en todo momento, y hacen que el día a día sea más distinto al otro.

A mi tutor M. Sc. Bayardo Bohórquez Escobar y al Coordinador de Titulación, M. Sc. Edwin Palacios Meléndez por saber guiarme y ayudarme en el desarrollo del trabajo de titulación y culminarlo con éxito.

A mis compañeros de aula, por compartir estos años en la Carrera de Telecomunicaciones y por hacer de este viaje una muy bonita experiencia.

Gracias a todos, los llevare en mi corazón siempre.

LA AUTORA

CABEZAS CHALCO, GLORIA PIEDAD

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ING. MIGUEL ARMANDO HERAS SÁNCHEZ, M. Sc.

DIRECTOR DE CARRERA

f. _____

ING. NÉSTOR ARMANDO ZAMORA CEDEÑO, M. Sc.

COORDINADOR DE ÁREA

f. _____

ING. LUIS SILVIO CÓRDOBA RIVADENEIRA

OPONENTE

Índice General

Índice de Figuras

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 2

Capítulo 3

Resumen

El desarrollo del trabajo de titulación consistió en realizar el análisis y evaluación de la tecnología ZigBee en aplicaciones de redes de sensores inalámbricos utilizando la comunicación P2P. Primero, se realiza las generalidades del trabajo, tales como, introducción, antecedentes, definición y justificación del problema a investigar, así como el objetivo general y objetivos específicos, hipótesis y metodología de investigación. Posterior, se describe los fundamentos teóricos de redes inalámbricas, redes oppnets (oportunistas) y ZigBee. En forma general, las redes inalámbricas son la mejor solución al momento de realizar transmisiones de datos de manera remota utilizando sensores para aplicaciones en comunicaciones punto a punto. Zigbee es una de las principales y más conocidas tecnologías de comunicación inalámbrica. Además de movilidad, característica típica de dispositivos inalámbricos, el Zigbee también posibilita dispositivos móviles de tamaño y peso reducido. Estas características, más el bajo consumo de energía alcanzado por dispositivos Zigbee, son esenciales en aplicaciones para las áreas de monitoreo remoto, control y sensoración, como por ejemplo para las redes WSN. Para poder realizar la parte final, se especifica los escenarios de simulación en Beacon y CSMA/CA. Finalmente, se desarrolla una interfaz gráfica (GUI) en MatLab que permitió modelar el comportamiento de la tecnología ZigBee mediante redes de sensores inalámbricos.

Palabras claves: COMUNICACIONES, INALÁMBRICAS, ZIGBEE, WSN, TOPOLOGÍAS, MATLAB.

CAPÍTULO 1: Descripción general del Trabajo de Titulación

1.1. Introducción.

Los sistemas de comunicaciones inalámbricos siguen siendo una de las redes de mayor uso en la transmisión de datos. Existen diferentes tecnologías de comunicación inalámbrica, tales como, Bluetooth, Xbee y ZigBee. Las dos últimas tecnologías son muy utilizadas en diversas aplicaciones de redes Ad-hoc móviles (MANETs) mediante dispositivos de sensores.

ZigBee es una tecnología emergente diseñada para bajo consumo de datos y bajo consumo de energía, y aplicaciones de bajo costo. El nombre "ZigBee" proviene de la danza en zigzag que utilizan las abejas para compartir información, como la ubicación, la distancia y la dirección de una fuente de alimento. El área de aplicación principal es redes de sensores inalámbricos *(Wireless Sensor Network, WSN)*, donde la energía es limitada (las baterías deben mantenerse durante años), el rango de transmisión puede ser pequeño y la velocidad de transmisión también puede ser pequeña. Lo interesante de ZigBee que también es ampliamente utilizado en domótica y control industrial.

ZigBee e IEEE 802.15.4 son protocolos basados en estándares que proporcionan la infraestructura de red necesaria para aplicaciones de redes de sensores inalámbricos. El estándar 802.15.4 define las capas físicas y control de acceso al medio *(Medium Access Control, MAC)*, mientras que ZigBee define las capas de red y de aplicación. La red ZigBee tiene un rango

de transmisión corto, normalmente entre 10 a 75 m, que depende en gran medida del ambiente en particular. La humedad, las interferencias y también las barreras intermedias pueden afectar el rango de transmisión.

ZigBee es ideal para redes de sensores inalámbricas principalmente debido a la implementación de una capa física (PHY) de baja potencia. En este diseño, ZigBee se permite operar en tres bandas ISM sin licencia: 868 MHz (Europa), 915 MHz (América del Norte) y 2,4 GHz (a nivel mundial).

Las WSNs son utilizadas especialmente para aplicaciones en tiempo real, plantean problemas fundamentales a la comunidad científica. Estos problemas están relacionados con el límite de los recursos energéticos y las limitaciones en tiempo real en el retraso de la comunicación. El buen funcionamiento de estas redes depende principalmente del resultado de la vida de la red de las energías de los nodos y del retraso de comunicación que debe cumplir los plazos requeridos. Por lo tanto, el diseño de pozos de redes de sensores inalámbricos en tiempo real debe ser con la predicción del consumo de energía y el retraso de la comunicación.

1.2. Antecedentes del problema a investigar.

La búsqueda de información relacionado al trabajo de titulación permite establecer la relación causa-efecto de las comunicaciones inalámbricas ZigBee a través de sensores. La mayoría de trabajos encontrados fueron

publicaciones en revistas y trabajos de grado. A continuación, se describen algunas investigaciones relacionados al tema propuesto.

1. El trabajo de (Ouni & Ayoub, 2013) propone un modelo analítico para predecir la vida útil y el retardo en redes de sensores inalámbricas IEEE 802.15.4/ZigBee. El modelo propuesto se basa en suposiciones realistas, es decir, que considera las características más importantes de la red, tales como, tiempos de inactividad de retroceso *(Backoff)*, escuchas e interferencias por colisiones y errores de transmisión. En comparación con los resultados de la simulación y otros enfoques analíticos, el modelo proporciona una predicción de vida y retardo de red confiable.
2. El trabajo de (Hwang & Yu, 2012) propone el diseño e implementación de un sistema de monitoreo y control remoto mediante redes ZigBee. Este sistema se dirige a una red doméstica. Los servicios web y un teléfono inteligente se utilizan para que el sistema del cliente supervise y controle el hogar

1.3. Definición del problema a investigar.

Necesidad de realizar el análisis y evaluación del protocol ZigBee en aplicaciones de redes de sensores inalámbricos utilizando comunicaciones punto a punto (conocido como P2P).

1.4. Justificación del problema a investigar.

Gracias al rápido desarrollo de la tecnología de la información y al crecimiento de Internet a través de redes de alta velocidad, los entornos de

red han cambiado de entornos de oficina basados en industrias empresariales e instituciones públicas hasta la interconexión de la electrónica digital en redes domésticas. Las aplicaciones basadas en la red doméstica son muy diversas y las áreas de monitoreo y control remoto han sido estudiadas.

Recientemente, ZigBee se ha convertido en una de las tecnologías más prometedoras para redes domésticas. ZigBee es una especificación para un conjunto de capas de software de redes, seguridad y aplicaciones que utilizan una tecnología de comunicación de baja velocidad y baja velocidad de datos basada en el estándar IEEE 802.15.4 para redes de área personal. Además, debido al rápido crecimiento de la tecnología móvil, los teléfonos inteligentes de alto rendimiento están muy extendidos y en casos cada vez mayores se utilizan como un dispositivo terminal.

1.5. Objetivos del problema a investigar.

1.5.1. Objetivo General.

Realizar el análisis y evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P.

1.5.2. Objetivos específicos:

- Describir la fundamentación teórica de redes inalámbricas con énfasis en la tecnología ZigBee y sensores inalámbricos.
- Modelar el protocolo ZigBee para aplicaciones de redes de sensores inalámbricos.

- Evaluar el desempeño de la red de sensores inalámbricos utilizando la tecnología ZigBee.

1.6. Hipótesis.

Si se realiza el análisis y evaluación de la tecnología ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones punto a punto y se comparan sus comportamientos, lo cual permitirá profundizar en el conocimiento de sus particularidades.

1.7. Metodología de Investigación.

De acuerdo a los autores Cortés C. & Iglesias L., (2004) la metodología de investigación permite a los investigadores dotar de una serie de conceptos, principios y leyes que permitan guiar de manera eficiente el proceso de investigación. También, habla de los enfoques metodológicos, que son: cuantitativos y cualitativos. Para el presente trabajo de titulación, se utiliza el enfoque cuantitativo, debido a que se basa en observaciones y evaluaciones de los fenómenos en cuestión, que es la tecnología ZigBee mediante el uso de sensores inalámbricos.

CAPÍTULO 2: Fundamentos teóricos.

2.1. Visión general de redes.

Este capítulo describe el estado del arte de las Redes Oportunistas conocidas como Oppnets empezando por enmarcar su definición en el ámbito de las redes inalámbricas y de las redes inalámbricas móviles. Se sigue la definición de los principales términos en el ámbito de las Redes Oportunistas permitiendo un mejor entendimiento de su funcionamiento.

2.2. Redes inalámbricas.

Las redes inalámbricas consisten en dispositivos que se comunican entre sí sin el uso de cables o hilos, y se clasifican de acuerdo con las diferentes exigencias en términos de alcance máximo, velocidad de transmisión de datos y entorno de aplicación. Las redes inalámbricas se clasifican (véase la figura 2.1) en:

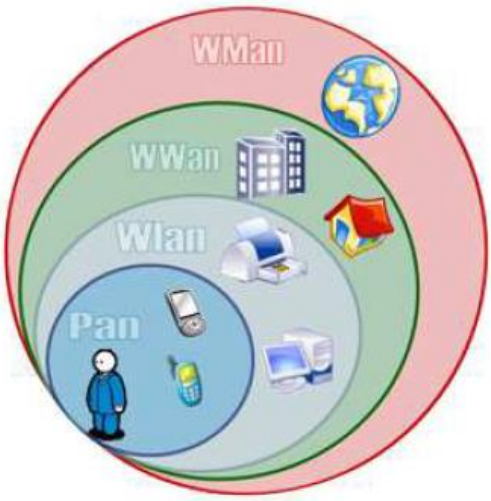


Figura 2. 1: Clasificación de redes inalámbricas.
Fuente: (Sharma & Dhir, 2014)

- Redes inalámbricas de área personal *(Wireless Personal Area Network, WPAN)* o de corta distancia: son redes muy utilizadas en comunicaciones punto a punto, pero también se pueden aplicar en comunicaciones punto a multi punto. La distancia entre dispositivos puede variar entre 1 y 10 metros con una velocidad de transmisión reducida (100 a 200 Kbps). Los próximos años se plantean futuros avances en cuanto a su utilización en entornos industriales. (Salazar Soler, 2016)
- Redes de área local inalámbrica *(Wireless Local Area Network, WLAN)*: son redes para aplicaciones muy específicas. La distancia entre dispositivos puede variar de algunas decenas en ambientes interiores y de algunos cientos en ambientes exteriores con una tasa de transmisión elevada (1 a 20 Mbps). Esta tecnología es especialmente utilizada en aplicaciones LAN y acceso a Internet mediante Hot-Spots que incluyen entornos no industriales. Actualmente se están desarrollando para ambientes industriales, que se plantean como muy robustas y reconfigurables. (Salazar Soler, 2016)
- Redes inalámbricas de área extensa *(Wireless Wide Area Network, WWAN)*: son redes muy utilizadas en comunicaciones punto a punto de larga distancia y con elevada tasa de transmisión (10 Mbps). (Salazar Soler, 2016)
- Redes inalámbricas de área metropolitana *(Wireless Metropolitan Area Network, WMAN)*: son redes que interconectan varias LANs geográficamente próximos con dudas importantes. Así, una MAN

permite que los dispositivos distantes se comuniquen como si formarán parte de una misma red local. Una MAN está formada por conmutadores o conmutadores interconectados por relaciones de alta velocidad. (Salazar Soler, 2016)

Los dispositivos utilizados en redes inalámbricas de acuerdo con cada una de estas clasificaciones pueden permanecer fijos en determinados puntos geográficos o, alternativamente, tener uno o varios dispositivos móviles. En este último caso se encuadran las redes inalámbricas móviles.

2.2.1. Redes inalámbricas móviles.

Se consideran redes inalámbricas móviles todas las redes que poseen uno o varios dispositivos móviles capaces de ser transportados entre puntos geográficos distintos y, por esa razón, la red presenta alteraciones frecuentes de distancia entre sus dispositivos. La distancia entre los dispositivos que desean comunicarse sin el uso de hilos es un factor importante, pues además de cierto alcance las comunicaciones se limitan. En otras palabras, las redes oportunistas (Oppnets) se encuadran en tipos de redes inalámbricas móviles en las que también se incluyen las redes de Mesh, Redes Ad-hoc, Redes Vehiculares y Redes de Sensores.

2.2.2. Redes Móviles Ad-hoc.

Conocidas por sus siglas en inglés *Mobile Ad-hoc NETworks*, o también llamadas MANETs, consisten en nodos móviles libres para describir

trayectorias arbitrarias. La designación Ad-hoc surge en el contexto de redes informales especificadas para una aplicación muy concreta, como por otra parte el propio término sugiere: "para esto" o "para esta finalidad". En la figura 2.2 se observan varios ejemplos de redes Ad-hoc.

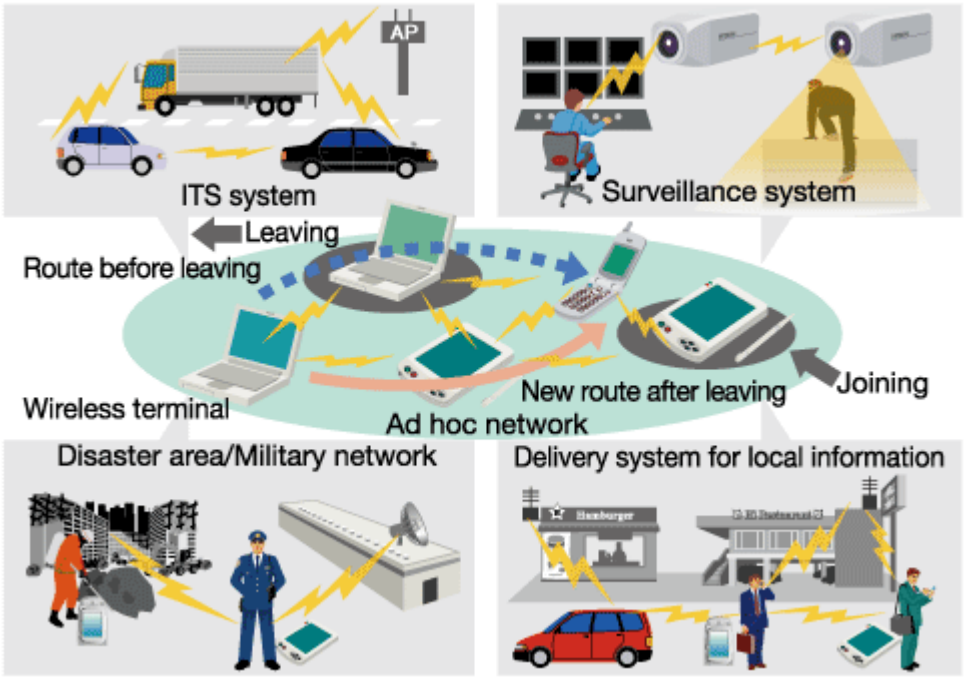


Figura 2. 2: Ámbitos de aplicación de redes Ad-hoc inalámbricas.
Fuente: (Ryaan, 2012)

Cada nodo tiene un transmisor omnidireccional definido por el protocolo IEEE 802.11 capaz de transmitir la señal a la zona geográfica circundante, que define una transmisión de rango o alcance de transmisión. El alcance de transmisión consiste en la zona geográfica afectada por la señal transmitida por un transmisor omnidireccional. Todos los nodos contenidos en el mismo alcance de transmisión se consideran nodos vecinos y son capaces de enviar y recibir mensajes entre sí. Uno de los nodos envía un mensaje que es escuchado por todos los nodos contenidos en el mismo alcance de

transmisión. La topología de esta red puede variar y en algunos casos ser dividida mediante la movilidad asignada a los nodos.

El uso de estas redes se complica cuando se pretende comunicar entre nodos fuera de la zona de vecindad pues requiere una difusión multi-hop (múltiples saltos) de los mensajes. En una difusión multi-hop, los mensajes se reenvían desde un nodo origen a un nodo destino a través de nodos intermedios, lo que implica una enorme ocupación de banda e incluso de consumo de energía de los nodos. Se añaden limitaciones a la movilidad de los nodos y la capacidad de almacenamiento.

2.2.3. Redes Inalámbricas Mesh.

Las Redes Inalámbricas Mesh *(Wireless Mesh Network, WMN)* conocidas como enmalladas, están constituidas por enrutadores enmallados y usuarios enmallados. Son conocidas como redes IEEE 802.11s fiables y de bajo costo. Típicamente los enrutadores Mesh están estáticos (o con movilidad muy reducida) formando una "espina dorsal" y permite que los usuarios enmallados accedan a la red. En la figura 2.3 se puede observar una topología de este tipo de red.

Al igual que en las MANETs, las WMNs permiten amplia cobertura geográfica, elasticidad y reducidos costos de acceso. La movilidad de la red depende de las características de los dispositivos asociados a los nodos. Por esta razón, es una topología ampliamente utilizada en redes WLAN. La

facilidad de configuración y expansibilidad son las principales ventajas del uso de redes WMN, siendo la escalabilidad a su principal limitación.

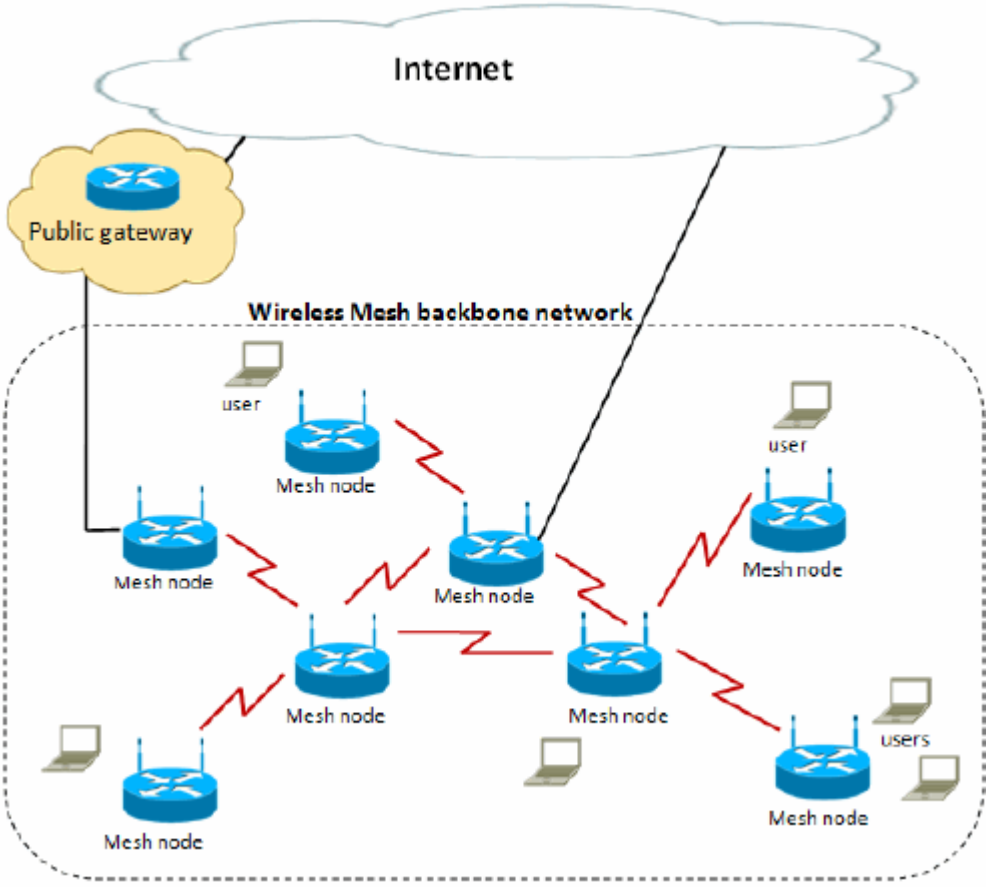


Figura 2. 3: Ejemplo de una red Mesh.
Fuente: (Seppänen, Kilpi, & Suihko, 2015)

El protocolo IEEE 802.11 utiliza el método de acceso múltiple por detección de portadora y prevención de colisiones *(Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA)* a la capa MAC y esto hace que la red WMN sufra las mismas interferencias que las redes MANETs. Las soluciones multi-radio y multi-canal minimizan el problema mientras la red reenvía información o mientras los usuarios enmallados pretenden acceder a determinadas funcionalidades.

Ambas soluciones permiten separar dos tipos de tráfico en el dominio inalámbrico, mientras que la red se configura y encamina información en un canal, los accesos de los usuarios enmallados a los servicios de la red transcurren en un canal diferente. Aunque, en las redes MANETs esta separación no se aplica, ya que las diferentes funcionalidades de la red se desarrollan en el mismo canal y, por esta razón, tienen una performance inferior a las WMN.

2.2.4. Redes Ad-hoc Vehiculares.

Las redes Ad-hoc vehiculares *(Vehicular Ad-hoc NETworks, VANETs)* son un conjunto de redes MANETs en las que los nodos se encuentran fijados en vehículos móviles. La principal particularidad de este tipo de redes es la velocidad de los nodos que es muy superior a lo que se espera en las MANETs simples. Por otro lado, son redes previsibles, siempre que los vehículos cumplan las rutas predefinidas.

La velocidad de los nodos implica un cambio frecuente de la topología de la red y, por otro lado, como los nodos se mueven en vehículos autónomos (con su propia alimentación), los recursos de una red VANET pueden ser abundantes. En la figura 2.4 se observa una representación posible de VANET dada por Eiza, Ni, Owens, & Min, (2013) en lo que se refiere a la diversidad de equipos y comunicaciones. Estas redes permiten la comunicación entre nodos fijos y nodos móviles, y entre un nodo móvil y fijo, según la necesidad.

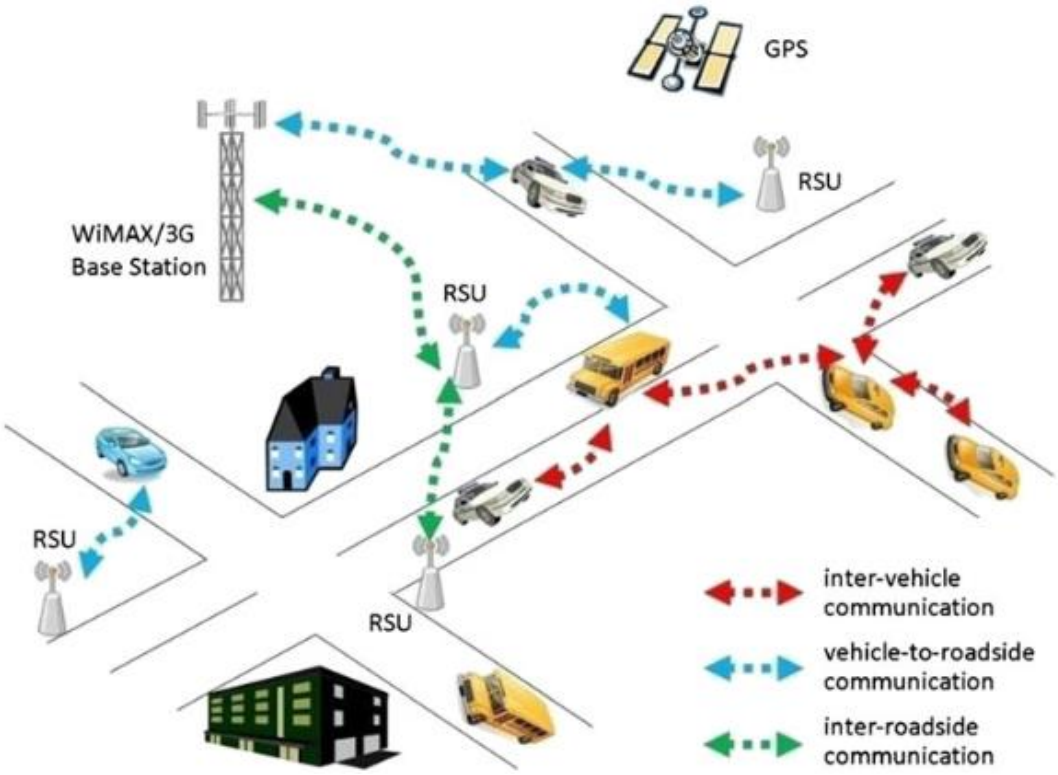


Figura 2. 4: Ejemplo de una red Ad-hoc vehicular.
Fuente: (Eiza et al., 2013)

2.2.5. Redes Inalámbricas de Sensores.

Las redes inalámbricas de sensores *(Wireless Sensor Networks, WSN)*, consisten en redes cuyos dispositivos se encuentran distribuidos en una zona geográfica considerable para monitorear y/o controlar un ambiente específico. Los nodos de los sensores son típicamente de bajo consumo, poseen gran capacidad de almacenamiento y se comunican entre sí a través de protocolos de comunicación específicos.

En particular, esta topología no está orientada a movimientos frecuentes por lo que pueden ser predefinidos, tal como se ilustra en la figura 2.5. El

intercambio de información es típicamente multi-hop en el que el retardo debe ser tomado en consideración.

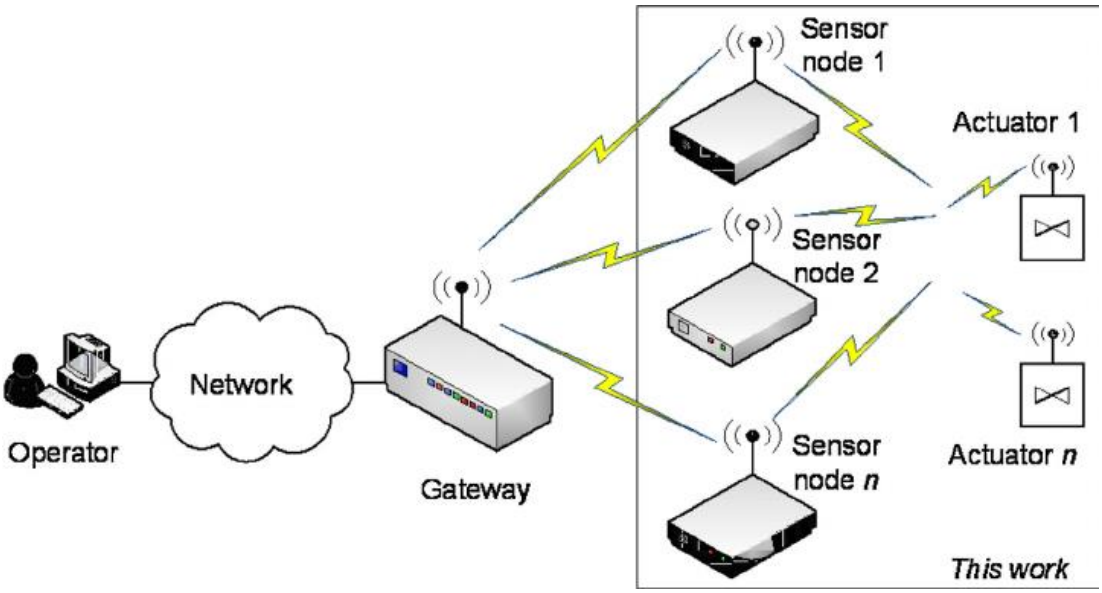


Figura 2. 5: Ejemplo de aplicación de una red inalámbrica de sensores.
Fuente: (Somov, Baranov, & Spirjakin, 2014)

En las redes tradicionales los nodos se comunican a través de estaciones de radio base, que constituyen una infraestructura de comunicación (ver figura 2.6).

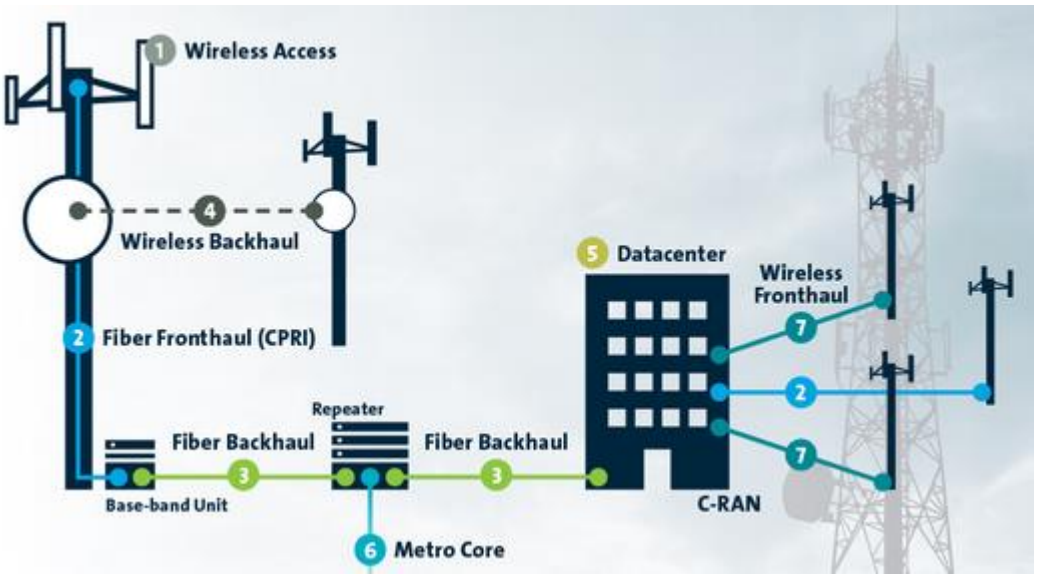


Figura 2. 6: Ejemplo de red tradicional estructurada.
Fuente: (Macom, 2016)

Según Khoukhi, Badis, Merghem-Boulahia, & Esseghir, (2013) en las redes MANETs los nodos intercambian información directamente entre sí como se muestra en la figura 2.7, por lo tanto, desde el punto de vista de la organización, las redes WSN y MANET son similares porque permiten la comunicación directa entre los nodos sin el uso de cableado.

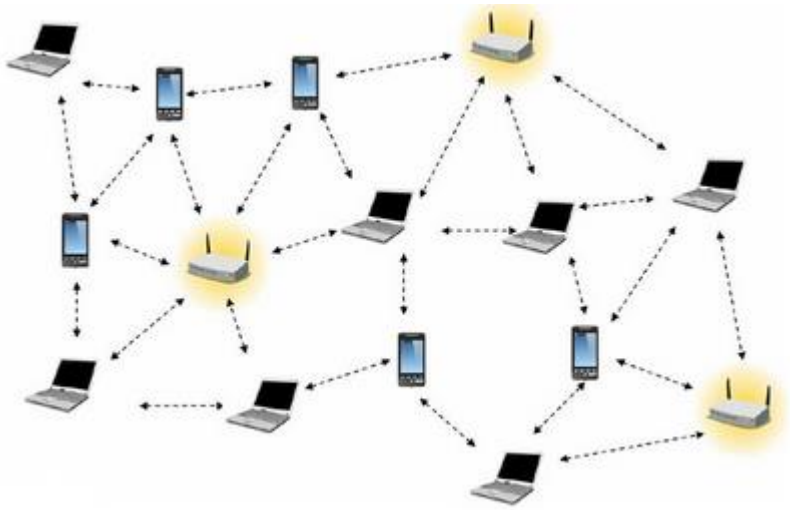


Figura 2. 7: Ejemplo de red no estructurada.
Fuente: (Khoukhi et al., 2013)

Sin embargo, las MANETs tienen como función básica proveer un soporte de comunicación entre los diferentes elementos computacionales que individualmente pueden estar realizando tareas distintas. Las WSN, a su vez, tienden a ejecutar una función colaborativa donde los elementos (sensores) provienen datos que son procesados por nodos especiales, llamados nodos sumideros *(sink nodes)*, los cuales pueden funcionar como:

- Fuente de datos *(Data Source)*: permite acciones de adquisición, procesamiento, memorización, comunicación sin cables, y actuación en el propio ambiente;

- Enrutador de datos *(Data Router)*: transmite la información de un nodo vecino a otro a través de la estación de control. La estación de control procesa y analiza la información recogida por los diferentes nodos/sensores de la red.

2.2.6. Redes Oportunistas.

Las redes oportunistas u oppnets, también conocidas como redes tolerantes de retardo *(Delay Tolerant Networks)*, corresponden a la interceptación de redes Ad-hoc, sistemas punto a punto (Peer-to-Peer, P2P) y WSN que mejoran las aplicaciones inalámbricas ya existentes y desencadenan el desarrollo de nuevas aplicaciones. Se trata de redes Ad-hoc que interconectan varios módulos sin cables a partir de nodos originarios siendo las conexiones, en general, temporales: uno o varios nodos originales invitan o simplemente abandonan otros nodos, según su utilidad para los servicios prestados por la red en un momento dado.

La topología de oppnets varía según la movilidad de los nodos, su activación y desactivación. Por lo menos, una oppnet tiene dos características:

a. Descubrimiento del nodo *(Node Discovery)*: permite que los nodos de la red busquen otros nodos que se encuentren en el mismo alcance de transmisión para establecer conexiones;
b. Cambio de salto único *(One-Hop Exchange)*: permite el intercambio de información entre los nodos conectados.

Las redes oportunistas difieren de las redes tradicionales, como las MANET o las WMNs, en lo que se refiere a la movilidad de los nodos y la capacidad de cambios frecuentes de topología de la red cuando se justifica en el marco de la aplicación. La comunicación entre los nodos de la red sólo es posible si se encuentran en el mismo alcance de transmisión.

Tienen la capacidad de auto-configurar y permiten detectar dispositivos vecinos usando medios de comunicación como ZigBee, Bluetooth, Wi-Fi, etc. Las oppnets tienen potencial en situaciones de emergencia, por ejemplo, catástrofes naturales. En los últimos años hemos visto grandes desastres, como el ataque terrorista del 11 de septiembre, el tsunami en el sudeste asiático, el huracán Katrina y el terremoto en nuestro país del 16 de abril del 2016. Las víctimas y los daños son demasiado a menudo agravados por los problemas que enfrentan los primeros socorristas y los trabajadores de las agencias de socorro. Hay un hilo común en todos estos problemas: falta de instalaciones de comunicación adecuadas en las áreas de desastre y más allá. Por lo tanto, proporcionar medios de comunicación seguros en situaciones de emergencia es un desafío fundamental para las tecnologías de comunicación e información.

2.3. Definiciones básicas de redes oportunistas.

En esta sección se definen los principales conceptos relativos a las redes oportunistas y aspectos a tener en cuenta en cuanto a la modelación de una red oportunista, así como a la integridad y seguridad de las mismas.

2.3.1. Nodo Móvil.

El Nodo o módulo de una red oportunista es un dispositivo dotado de capacidad de comunicación inalámbrica que utiliza protocolos para compartir y diseminar información. Si un nodo tiene movilidad en oppnet se denomina "Nodo móvil".

2.3.2. Ayudantes de oppnet.

Los ayudantes de redes oportunistas *(Oppnets helpers)* son aquellos que no tienen la capacidad de detección, pero pueden contribuir positivamente a la oppnet en lo que respecta a la habilidades y capacidades de comunicación, procesamiento y detección (sensores). Cuando la oppnet trabaja en modo "desaster", es decir, en un modo de operación particular, no requiere funcionalidades adicionales a las que realmente necesita en el modo actual y, por lo tanto, prescinde de los oppnets helpers que no son necesarios.

2.3.3. Modelización de redes oportunistas.

La modelación de Oppnets para una determinada aplicación debe atentar determinados aspectos en los que se destacan:

- Servicio de reconocimiento de presencia *(Presence Awareness Service)*: proporciona a la aplicación la información de los nodos y de los usuarios que están activos en el mismo alcance de transmisión;
- Servicio de intercambio de mensajes *(Message Exchange Service)*: permite que los mensajes se intercambien entre los nodos del mismo alcance de transmisión (este servicio implementa las comunicaciones

one-hop). Aunque, este servicio, no verifica el éxito o fracaso con que los mensajes se recibieron en el destino. Esta tarea está destinada al servicio Acknowledgement perteneciente al nivel de aplicación;

- Servicio de filtrado de información *(Information Filtering Service)*: permite que cuando la oppnet esté en peligro de SPAM, la información irrelevante se filtre para que sea transparente para el usuario. La autenticidad de la información queda así asegurada a través de una firma digital;
- Servicio de distribución de información *(Information Distribution Service)*: no contempla la participación del usuario, ésta puede decidir si desea compartir o restringir el uso de los recursos del dispositivo;
- Servicio de seguridad *(Security Service)*: para mantener la integridad y la autenticidad de las comunicaciones, los servicios de seguridad ofrecen una firma y encriptación de información;
- Servicio de gestión de identidad *(Identity Management Service)*: especifica cómo el usuario está en el sistema. El usuario puede interactuar de forma anónima, con un pseudónimo o con una firma propia. En el caso de mantener el anonimato los servicios deben proteger la información de todas las capas de comunicación, de lo contrario pueden ser atacadas y eventualmente destruidas.
- Servicio de notificación de usuario *(User Notification Service)*: notifica al usuario en caso de producirse información inadecuada. La implementación de este servicio depende de las capacidades del dispositivo y de la urgencia de las notificaciones.

El diseño de la aplicación de una red oportunista debe atenderse de acuerdo a la siguiente estructura (véase la figura 2.8): (a) colaboración activa *(Active Collaboration)* se ocupa de la proximidad física del usuario y tiene la ventaja de permitir un conocimiento completo de las responsabilidades del usuario en los dispositivos de la red. Mientras que, la colaboración pasiva *(Passive Collaboration)* es una forma de recoger y transmitir cualquier información entre usuarios en el mismo alcance de transmisión y se desarrolla sin la intervención del usuario.

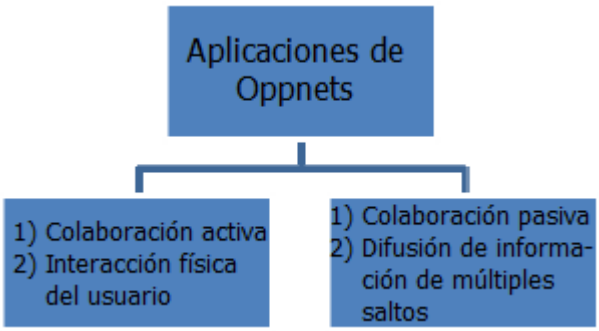


Figura 2. 8 Aplicación de Red Oportunista.
Fuente: (Heinemann, 2007)

La diseminación de información es el proceso por el cual la información es distribuida por la red oportunista. Las reglas se especifican en los protocolos de intercambio de información y se desvelan en dos pasos: (a) descubrimiento del nodo *(Node Discovery)*, y (b) Cambio de salto único *(One-Hop Exchange)* presentados en la sección anterior. Son los nodos de la oppnet que definen el modelo del sistema de la red oportunista.

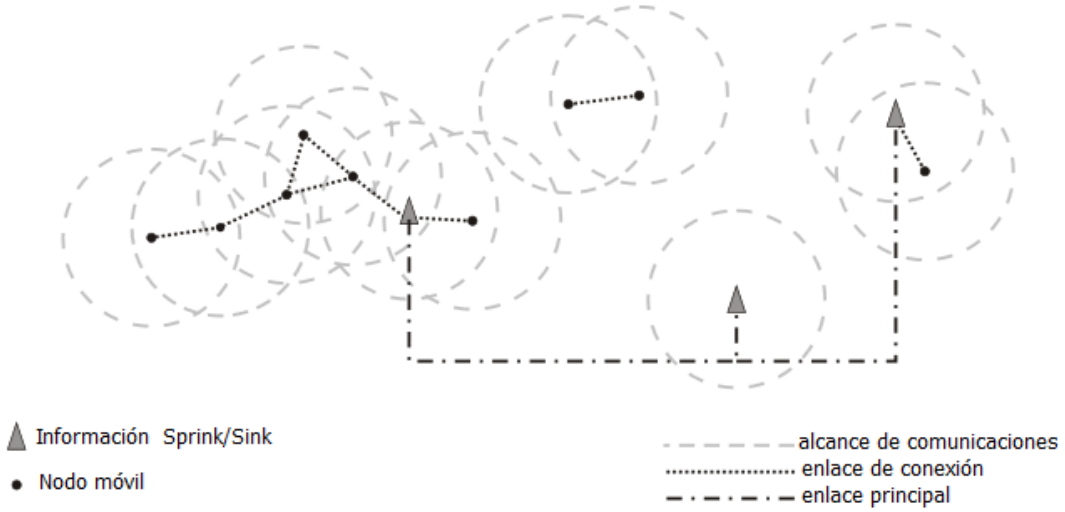


Figura 2. 9 Modelo del sistema para la diseminación de datos.
Fuente: (Heinemann, 2007)

La figura 2.9 representa un modelo posible de la diseminación de datos, donde se representan varios nodos móviles con su alcance de transmisión típicamente esférico. Cabe señalar que en la práctica no es exactamente una esfera, ya que la señal irradiada sufre interferencias de diferentes direcciones.

2.3.4. Privacidad y Seguridad.

Uno de los problemas de privacidad y seguridad de redes oportunistas es el hecho de que la autenticidad, en general, no puede ser configurada cuando los dispositivos se unen a la red. Por lo tanto, no es posible garantizar que los dispositivos maliciosos no se unen. Distribuir claves de seguridad sólo a los dispositivos considerados "no maliciosos" es muy complicado en entornos Ad-hoc.

Por otro lado, permitir mecanismos de autenticación basada en encriptación no ayuda en todas las situaciones. La figura 2.10 muestra el

esquema de seguridad de una oppnet cuando un nuevo oppnet helper se une a la red. En ausencia de mecanismos de autenticación inicial, todos los pasos de la figura 2.10 son obligatorios. El cifrado es una forma de proteger la información de oppnet. Un controlador transmite su clave a todos los dispositivos y todos ellos encripta su información basada en la clave pública suministrada. El controlador posteriormente descifra la clave privada resultante de cada dispositivo cuando dicha acción esté justificada.

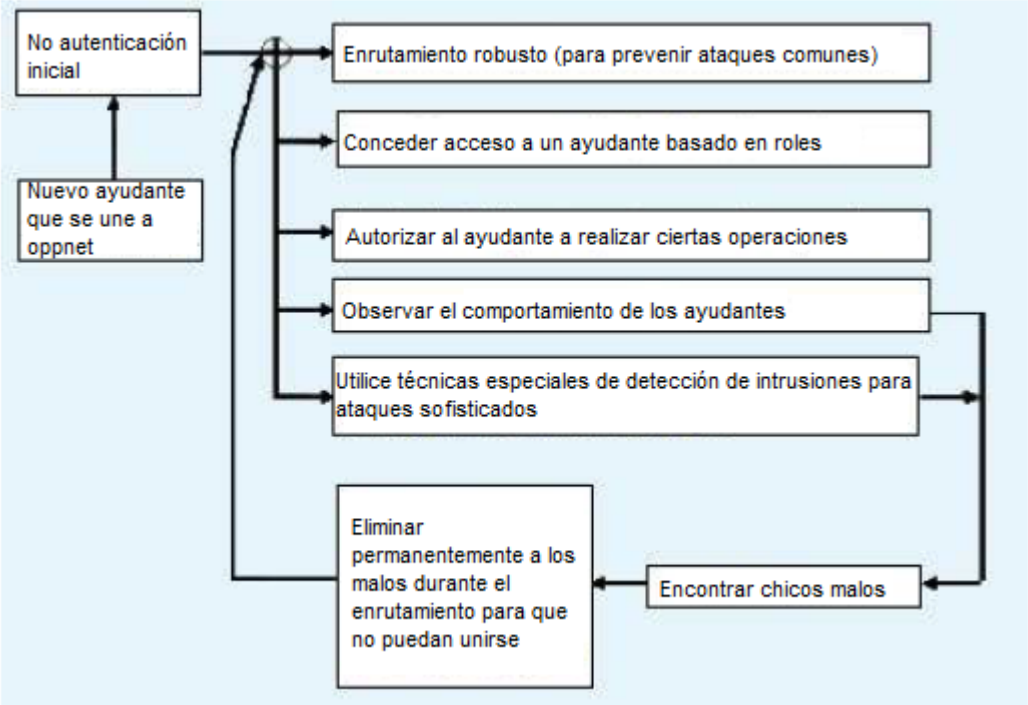


Figura 2. 10: Esquema de seguridad en la adición de nuevo oppnet helper.
Fuente: (Lilien, Kamal, Bhuse, & Gupta, 2007)

Para mantener la integridad de la información se utilizan firmas digitales que se revelan cómodamente, aunque costosas para dispositivos limitados tanto en procesamiento como en consumo de energía. Por otro lado, el tamaño de los paquetes también varía a lo largo de la red para facilitar la transmisión, por lo que los procesos de fragmentación y agregación deben ser

minuciosos en términos de seguridad. En caso contrario, la seguridad de la red está comprometida.

En resumen, oppnet puede ser fiable si la privacidad de sus oppnet helpers está garantizada a través de un control de acceso (autenticación y autorización) y de prevención de intrusiones (primitivas de intrusión). El control de accesos en el contexto de las Oppnets es más difícil de garantizar en comparación con Internet o redes Ad-hoc sobre todo debido a su heterogeneidad.

2.4. Ciclo de vida de las redes oportunistas.

Una red oportunista se basa en un principio fundamental: crece a partir de su semilla. La semilla de una oppnet consiste en el conjunto inicial de módulos predefinidos en el momento de su aplicación. El crecimiento de la red se produce mediante la detección de módulos vecinos y las invitaciones a los candidatos potenciales a ingresar a la oppnet. Los módulos detectados se identifican y se evalúan para averiguar su confiabilidad y utilidad para la oppnet. A continuación, se invita a los candidatos potenciales a adherirse a oppnet que pueden aceptar o rechazar. Una vez aceptada la invitación, el nuevo módulo (y sus recursos) pasan a formar parte de la red. Un participante de la red puede ser autorizado a realizar invitaciones a otros módulos para adherirse a la red.

Cuando un participante de oppnet deja de ser necesario, es decir, cuando se cumple su misión en la red, debe ser liberado y restaurado para el estado en que se encontraba antes de adherirse a ella. Esta particularidad minimiza la intromisión de dispositivos que ya no son necesarios en las tareas que la red se está ejecutando. Esta particularidad revela, además, el carácter oportunista de la red: sólo utiliza los servicios de un dispositivo mientras éste puede ser útil; caso contrario lo libera.

Los dispositivos de las redes inalámbricas oportunistas proporcionan acceso a comunicaciones distintas, estaciones remotas de adquisición, poder computacional y de almacenamiento de la información recopilada, así como otros recursos que sin ellos la red no tendría tal capacidad. En particular, los oppnets pueden establecer puentes entre medios de comunicación distintos y una forma de interconectar diferentes recursos y servicios. La generación de invitaciones se cancela cuando la oppnet destinada a una determinada aplicación tiene los oppnets suficientes para que permitan detectar, procesar y establecer comunicaciones entre los nodos. De esta forma, oppnet no está enviando invitaciones a los dispositivos, dejando este procedimiento sólo cuando se justifica.

2.5. Arquitecturas de comunicación.

2.5.1. Redes oppnets y Ad-hoc móvil.

Los nodos de una red oportunista se pueden fijar en estructuras móviles. En este aspecto, las redes oportunistas están intrínsecamente ligadas a las

MANETs, sólo que, desde el punto de vista de la capa de red, las MANETs están para la capa de red tal como los oppnets están para la capa de aplicación. En particular, una importante diferencia entre ambas consiste en el encaminamiento de información o enrutamiento.

Las MANETs enfocan los algoritmos de encaminamiento eficientes. Los más prometedores son el modo proactivo y reactivo. Son comunes soluciones que incluyen la posición geográfica de los nodos. En este contexto, desde que las MANET se han estudiado tanto en el ámbito de las aplicaciones militares, en respuesta a emergencias, ya en redes de sensores móviles, se asume siempre que, todos los nodos se relacionan entre sí, confían entre sí y comparten un objetivo común en la red.

A su vez, los oppnets están formados por grupos anónimos de dispositivos. Esto revela un impacto importante en el encaminamiento de información. Por ejemplo, en la figura 2.11 se muestra tres nodos posibles donde A se encuentra en el mismo alcance de transmisión que el nodo B, pero no se encuentra en el mismo alcance de transmisión que el dispositivo C, y, por otro lado, el nodo B si se encuentra en el mismo alcance de transmisión que el nodo C. Si el nodo A pretende comunicarse con el nodo C, toda la información pasará por el nodo B.

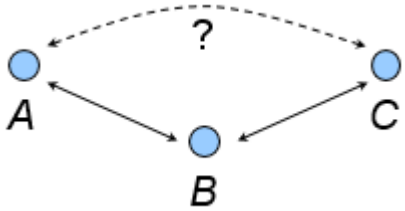


Figura 2. 11: Situación hipotética de transmisión de mensajes.
Fuente: (Heinemann, 2007)

Ahora, si los nodos no se conocen se plantean las siguientes cuestiones:

- ¿Por qué el nodo B está motivado a establecer la comunicación entre el nodo A y C? ¿Tiene sentido accionar (y consumir su batería) sólo para establecer el puente entre dos nodos (A y C)?
- ¿Por qué deben los nodos A y C confían en el nodo B para establecer la comunicación entre ambos? El nodo B puede fácilmente manipular o simplemente rechazar el mensaje.

No es sencillo encontrar la respuesta a estas cuestiones. Sin embargo, los modelos más recientes de las redes oppnets, proponen un esquema de comunicación de salto único (one-hop) donde el intercambio de mensajes entre nodos se hace entre los nodos que se encuentren directamente conectados. Adicionalmente, se aplican técnicas de preservación de la seguridad de los mensajes intercambiados.

2.5.2. Redes oppnets y Peer-to-Peer

Los sistemas Peer-to-Peer, o P2P, han levantado un alto interés en las comunicaciones. Se trata de arquitecturas de redes distribuidas donde los participantes comparten sus propios recursos de hardware. Este recurso es

necesario para proporcionar varias características a la red. Los recursos son accesibles entre sí, mientras que la comunicación entre dos dispositivos no necesita pasar por dispositivos intermedios. El primer aspecto que tienen en común las redes oppnets y las redes P2P, es la integración de las funcionalidades del cliente y del servidor en un único nodo o Peer. El nodo de una red oppnet consume y publica información. Sin embargo, la movilidad de los nodos no se considera en las redes P2P, ya que el principal objetivo de estas redes es compartir recursos y mecanismos.

Mientras, que en las MANETs y redes oppnets, la conexión entre los dispositivos se define automáticamente, por lo que son imprevisibles. Identificar y asignar recursos son servicios compartidos por dos nodos lo que implica un comportamiento cooperativo entre ambos. Pero en redes P2P móviles, el compartir recursos plantea cuestiones en cuanto a incentivos, confianza y reconfiguración. Finalmente, se puede concluir que la gama de aplicación de redes móviles P2P se basa en redes de teléfonos móviles y vehículos con capacidad de comunicación inalámbrica.

2.6. Principales tecnologías inalámbricas aplicadas.

En esta sección se introducen las tecnologías de comunicación inalámbrica más utilizadas en el mercado, en particular las que utilizan los estándares IEEE 802.11, IEEE 802.15 e IEEE 802.16. Estas tecnologías se encuentran actualmente integradas en dispositivos móviles de la plataforma y están disponibles para redes oppnets.

2.6.1. Estándar IEEE 802.11.

El estándar IEEE 802.11 se centra en los dos niveles inferiores del modelo OSI: la capa física (PHY) y la capa de conexión de datos (MAC) y especifica las tecnologías WLAN. La familia 802.11 incluye seis técnicas de modulación. Las tecnologías más populares son: IEEE 802.11a, IEEE 802.11b y IEEE 802.11g.

El estándar IEEE 802.11b transmite en la banda de frecuencia de 2.4 GHz con una velocidad de transmisión de 11 Mbps usando espectros ensanchados por secuencia directa *(Direct Sequence Spread Spectrum, DSSS)*. El estándar IEEE 802.11g, como el anterior, transmiten en la banda de frecuencias 2.4 GHz con una velocidad de transmisión de 54 Mbps usando DSSS o la multiplexación por división de frecuencias ortogonales *(Orthogonal Frequency Division Multiplexing, OFDM)*. En consecuencia, estos pueden interferir entre sí e incluso con otras aplicaciones que utilizan la misma banda de frecuencia (por ejemplo: teléfonos, dispositivos bluetooth, etc.).

El estándar IEEE 802.11 utiliza la banda 5 GHz y por eso no interfiere con los dispositivos en la banda 2.4 GHz, por otro lado, tiene una tasa de transmisión de 54 Mbps usando OFDM.

2.6.2. Estándar IEEE 802.15.4.

El estándar IEEE 802.15 es utilizado en la tecnología de redes inalámbricas de área personal *(Wireless Personal Area Network, WPAN)*.

Otras tecnologías más utilizadas son: (a) estándar IEEE 802.15.1 que se emplea en la tecnología Bluetooth, (b) estándar IEEE 802.15.3 empleado en banda ultra ancha *(Ultra WideBand, UWB)*, que especifica las capas MAC y PHY para altas tasas de transmisión (11 – 55 Mbps), y (c) estándar IEEE 802.15.4 empleado en la tecnología ZigBee, que especifica la capa PHY y MAC para bajas tasas de transmisión.

Por ejemplo, Bluetooth consiste en una tecnología de comunicación inalámbrica de forma segura diseñada para WPAN. Ha sido especificada por la cooperación especifica de Bluetooth establecida por Sony Ericsson, IBM, Intel y Nokia en 1999. Es una tecnología robusta, de bajo consumo y de bajo costo. Cada dispositivo puede comunicarse directamente con ocho dispositivos. A pesar de ser una tecnología de bajo consumo, la durabilidad de la batería depende del dispositivo en el que está embebido. Por ejemplo, el servicio Bluetooth de los teléfonos móviles sólo se puede suministrar mientras su batería permite que este dispositivo esté activo.

Bluetooth opera en la banda no licenciada en áreas Industrial, Científica y Médica (Industrial, Scientific and Medical, ISM) para uso no comercial. La frecuencia de operación está entre 2.4 GHz y 2.485 GHz en una señal Full-Duplex a la tasa nominal de 1600 saltos/s. Además, Bluetooth ha desarrollado capacidad para reducir la interferencia entre las tecnologías inalámbricas que comparten el espectro de 2.4 GHz. En aplicaciones con oppnets, la clase 2 de

Bluetooth puede ser utilizada siempre que la distancia entre los dispositivos sea de aproximadamente 10m.

Por otra parte, UWB consiste en una tecnología inalámbrica que ofrece un sistema de comunicación de banda ancha que soporta altas tasas de transferencia de datos, vídeo digital y streaming de audio. Se ha lanzado con el objetivo de sustituir los hilos de conexión de componentes electrónicos domésticos de alta fidelidad que requieren una transmisión superior a 1 Mbps y bajos consumos de potencia. Se basa en el estándar IEEE 802.15.3, es una tecnología de corto alcance (hasta 70 m) y de altas velocidades (hasta 55 Mbps). IEEE 802.15.3 sólo especifica las capas PHY y MAC, mientras que UWB llena las siguientes capas dejando la capa de aplicación libre al usuario. El estándar IEEE 805.15.4 será desarrollado mediante simulación en GUI de MatLab.

2.6.3. Estándar IEEE 802.16.

Para redes de gran alcance y alta velocidad existe el estándar IEEE 802.16 (WiMAN pero comercializado como WiMAX) que consiste en una colección de estándares típicamente utilizados en una tecnología WMAN: IEEE 802.16a (WiMAX) y especifica las capas PHY y MAC del modelo OSI. En la tabla 2.1 se pueden comparar las características más importantes en el momento de la elección de la tecnología inalámbrica. No obstante, la elección de la tecnología que mejor se adapte a la aplicación que se pretende realizar depende mucho de los requisitos de esa misma aplicación.

Así, para ambientes que se encuadren en la descripción de redes WPAN (corta distancia, baja tasa de transmisión) podemos utilizar las tecnologías ZigBee, Bluetooth y Wibree (englobando ambientes industriales y no industriales). En el caso de redes WLAN, en las que se requiere una tasa de transmisión y un alcance superior a las redes WPAN, se aconseja la tecnología Wi-Fi (801.11b y 802.11g).

Para las redes WWAN, definidas por la necesidad de transmitir a larga distancia y la elevada tasa de transmisión, las tecnologías que mejor se adecuan son claramente las tecnologías de comunicación móvil, por ejemplo, GPRS, y las tecnologías WiMAN y WiMAX definidas por los estándares IEEE 802.16.

Tabla 2. 1: Comparación de las tecnologías inalámbricas.

Estándares	ZigBee/IEEE802.15.4	Bluetooth	IEEE802.11 b/g	UWB
Frecuencia de operación	868/915 MHz, 2.4 GHz	2.4 GHz	2.4 GHz	3.1-10.6 GHz
Distancia (m)	30 a 70	10 a 30	30 a 100+	~10
Velocidad de transmisión	20/40/250 kbps	1 Mbps	2 a 54 Mbps	100+ Mbps
Número de dispositivos	55 a 65	8	50-200	
Consumo	~ 1mW	~40 a 100 mW	~160 mW a 600 W	~80 a 300 mW

Elaborado por: Autor.

Se prevé que pronto surjan soluciones más flexibles, más optimizadas para los recursos disponibles, más autónomos y, sobre todo, más baratos y masificados en el mercado, permitiendo que de una forma sencilla y casi

inmediata se consiga establecer comunicaciones entre los más variados dispositivos.

2.7. Introducción a ZigBee.

El estándar ZigBee fue desarrollado para servir de alternativa de comunicación inalámbrica en sistemas no muy complejos, desde el punto de vista de implementación de la red de comunicación, que exigen soluciones de bajo costo y bajo consumo de energía. Se trata de una tecnología de aplicación simple, que opera a través de protocolos de transferencia de paquetes de datos con características específicas, ofreciendo así flexibilidad en cuanto al tipo de dispositivo que puede ser controlado.

El $ZigBee$ surgió de la falta en el mercado de una norma que regulaba aplicaciones de redes inalámbricas para control y monitoreo de dispositivos, que ofreciese al mismo tiempo autonomía, seguridad y confiabilidad en el intercambio, creada por una alianza entre empresas del ramo de tecnología llamada $ZigBee$ Alliance, De información.

De esta necesidad se creó el estándar basado en la norma IEEE 802.15.4, homologada en mayo de 2003, donde se propuso la reglamentación para la conexión de dispositivos de radio con baja tasa de transferencia en PAN (Personal Area Network) y su operación en franjas libres de frecuencia. Entre las principales características de $ZigBee$, las que le concedieron

destaque en la automatización de procesos y consecuentemente llevaron su introducción en el mercado fueron:

- Reducir el consumo de energía ($low\ power$);
- Pila de protocolos de fácil implementación, conduciendo a interfaces de bajo costo ($low\ cost$);
- Capacidad para mantener un gran número de nodos por red (65.535 para cada Coordinador $ZigBee$);
- Admite diferentes topologías de red: estrella; Malla o clúster de árbol;
- Tiempo de conexión a red, rapidez en el paso del modo de espera al modo activo y de baja latencia ($low\ latency$);
- Dos modos de funcionamiento: la red de balizamiento y no balizamiento;
- Alta seguridad y confiabilidad, con capacidades de encriptación de 128 bits;
- Soporte a dos clases de dispositivos en una misma red definidos por el estándar IEEE 802.15.4, que son:
- (FFD) - puede funcionar en cualquiera que sea la topología de la red, desempeñando la función de coordinador de la red y consecuentemente tener acceso a todos los demás dispositivos. Son dispositivos de construcción más complejos.
- Reduced Function Device (RFD) - está limitado a una configuración con topología en estrella, no pudiendo actuar como coordinador de la red, pudiendo apenas comunicarse con ella. Son dispositivos de construcción más simples.

Soporte para tres tipos de dispositivos lógicos:

- Coordinador (Coordinador) - Asociado a los dispositivos del tipo FFD. Sus funciones son formar la red y asignar direcciones a los end points. Sólo hay uno por red;
- Enrutador (Router) - Asociado a los dispositivos del tipo FFD. Permite más nodos se unan a la red, aumentando su alcance físico. También puede realizar funciones de control y monitoreo. Su existencia es opcional;
- Dispositivo final - Asociado a los dispositivos del tipo RFD o FFD, efectúa acción de control y monitoreo a través de equipos acoplados a él tales como sensores, controladores, actuadores y otros.

2.8. Topologías

Las especificaciones de la norma IEEE 802.15.4, permiten tres tipos de topologías a ser implementadas de acuerdo con la aplicación. Todas las tres se describir con más detalle en esta sección.

2.9.1. Estrella (Star)

En la topología estrella (ver figura 2.12), la comunicación se establece entre los dispositivos y un único coordinador en la red. El coordinador obligatoriamente debe estar en modo de recepción cuando no esté transmitiendo para poder administrar todos los dispositivos finales. Se puede programar junto con microcontroladores de bajo costo y ser alimentados por una fuente continuamente.

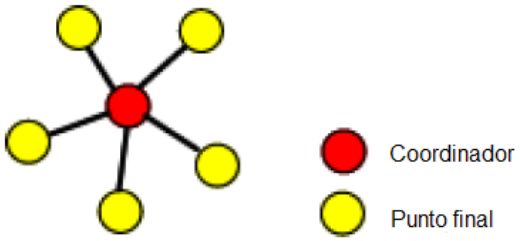


Figura 2. 12: Topología en la estrella.
Fuente: (Pathak, Kumar, Mohan, & Kumar, 2015)

Los demás dispositivos de la red pueden ser conectados a través de baterías usando o no microcontroladores. Este tipo de topología comúnmente se aplica en actividades de automatización residencial, periféricos de ordenador personal, juegos y aplicaciones médicas.

2.9.2. Árbol (Cluster Tree)

Esta topología en árbol (ver figura 2.13) se obtiene mediante la modificación de la topología en estrella, por la inclusión de nuevos dispositivos FFD que desempeñan la función de routers. Esto hace posible extender geográficamente la red. La distribución de datos y mensajes de control se lleva a cabo de una manera jerárquica en la que el coordinador llega a todos los puntos finales indirectamente por el uso de enrutadores.

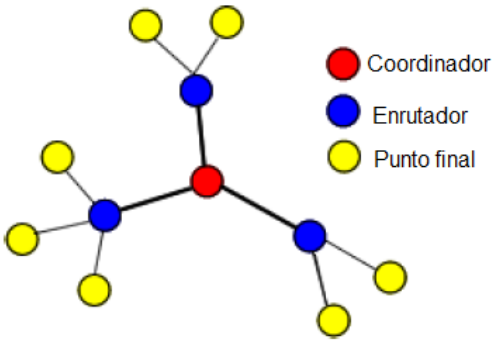


Figura 2. 13: Topología en clúster o árbol.
Fuente: (Pathak et al., 2015)

2.9.3. Malla (Mesh)

En una topología de malla (véase la figura 2.14), todos los dispositivos de tipo SD se comunican directamente, esto permite además de la expansión geográfica, también obtenido por la topología de árbol, la posibilidad de redundancia de red. Esto es útil, pues si un router pierde conexión con el coordinador todavía es posible controlarlo por el uso de otra ruta.

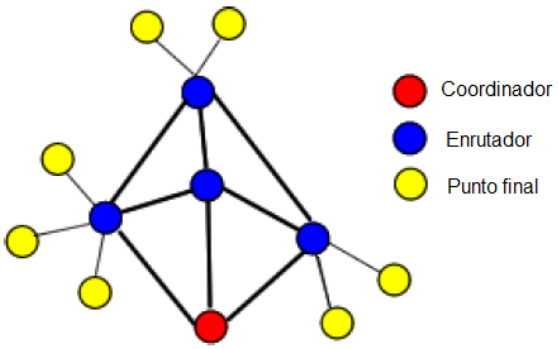


Figura 2. 14: Topología en malla.
Fuente: (Pathak et al., 2015)

2.9. ZigBee y el modelo OSI.

La arquitectura de las redes $ZigBee$ se basa en el modelo en capas OSI (ver figura 2.15). Cada capa es responsable por parte del estándar, ofreciendo servicios a las capas superiores. Las capas MAC y PHY se definen por la norma IEEE 802.15.4 y las superiores son definidas por la ZigBee Alliance. La capa PHY es la más baja en la jerarquía y tiene la función de permitir la transmisión y recepción de datos. Es en ella que se encuadran los circuitos electrónicos que hacen los intercambios de informaciones, que en el caso de las redes $ZigBee$ son los módulos transceptores de radiofrecuencia.

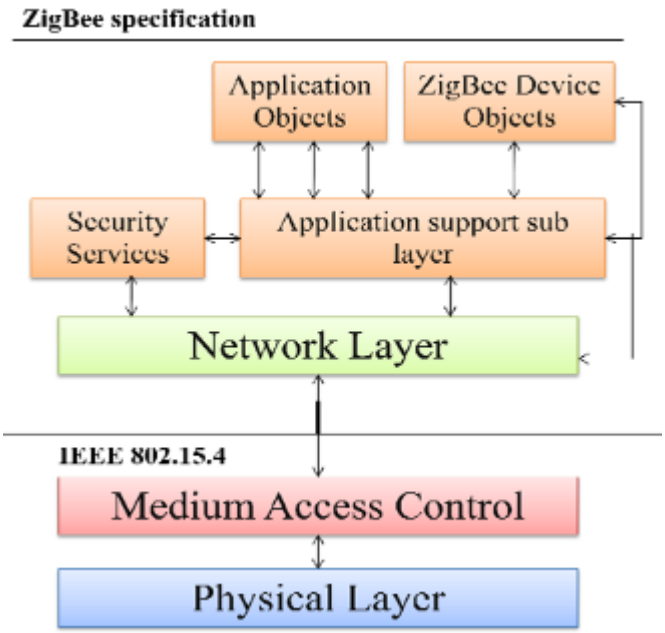


Figura 2. 15: Relación de la arquitectura protocolar del ZigBee con el modelo OSI. Fuente: (Kaushal, Kaur, & Kaur, 2014)

La capa MAC es responsable de controlar el acceso a los canales de radiofrecuencia, utilizando CSMA/CA. Además, especifica los tipos de dispositivos permitidos en la red, garantizando la seguridad de operación. Las demás capas de aplicación se encargan de asegurar una correcta gestión y soporte para las diversas aplicaciones del ZigBee.

2.9.1. La Capa PHY

Esta capa define cómo los dispositivos $ZigBee$ deben comunicarse a través de un canal inalámbrico. En una banda de frecuencia ISM (Industrial, Scientific, Medical) que no requieren licencias para ser utilizadas, siendo una de 2.4GHz utilizada en todo el mundo, una de 868MHz utilizada en Europa y una 915MHz utilizada en América del Norte.

Estas bandas de frecuencia difieren unas de otras debido a las características presentadas en la tabla 2.2.

Tabla 2. 2: Diferencias entre bandas de frecuencia ZigBee

Banda	Convergencia	Tasa de transferencia	Canales soportados	Aplicación recomendable
2.4 GHz	Mundial	250 kbps	16	Ambientes internos, menor distancia
868 MHz	Europa	20 kbps	1	Entornos externos, mayor distancia
915 MHz	Américas	40 kbps	10	Entornos externos, mayor distancia

Fuente: (Kaushal et al., 2014)

2.9.2. La Capa de Enlace

La subcapa MAC se ocupa de todos los accesos al canal de radio físico y es responsable de las siguientes: generación y sincronización balizas (paquetes de control que delimitan tramas utilizadas por el coordinador para sincronizar con otros dispositivos de la red); asociación de apoyo / disociación de dispositivos de la red; soportar el dispositivo de seguridad; Acceso a través de la gestión de canales CSMA/CA y proporcionar la validación y el reconocimiento de mensajes recibidos por la red.

Una red ZigBee puede utilizar dos mecanismos de acceso a los canales conocidos por beaconned y non-beaconned.

- Beaconned:

  En este modo, una portadora fragmenta la transmisión/recepción de datos en intervalos de tiempo denominados superficies delimitadas por beacons. Mientras que ninguna superficie está activada la red

permanece inactiva (stand by). En ese período, cualquier dispositivo que desee transmitir información tiene necesariamente que esperar su fin.

En situaciones donde hay más de un dispositivo transmitiendo al mismo tiempo, nuevos intentos deben hacerse por tanto al éxito, de lo contrario, se genera un mensaje de error de conexión.

En la figura 2.16 se presenta el esquema de una transmisión beaconned con tres radios, un coordinador y dos dispositivos finales. La señal de color azul es el faro de ella limitase el periodo de baliza, que es la unión del período supe trama con el período en que la red se mantiene en la pelea.

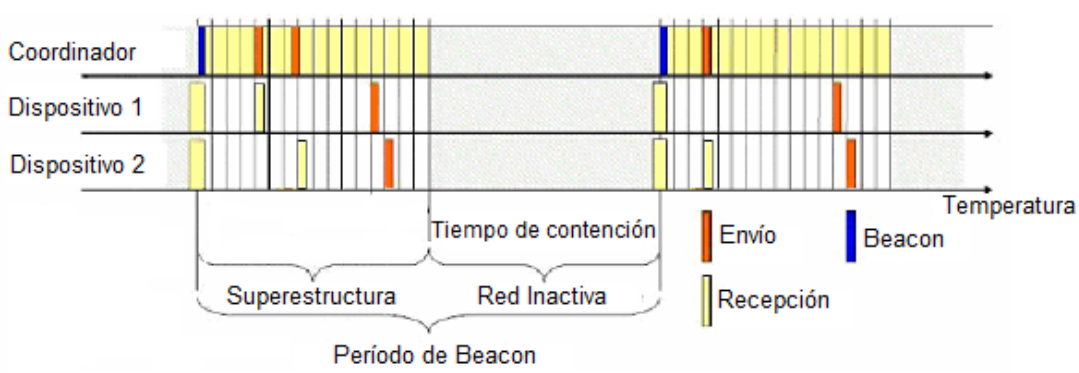


Figura 2. 16: Representación de una red social
Fuente: (Kaushal et al., 2014)

- No beaconned:

  Este modo funciona de la misma manera que el anterior, excepto que la transmisión es continua, sin tiempo de retención. La figura 2.17 muestra un esquema de este tipo de transmisión. Se envía sólo un beacon para iniciar la red y las transmisiones, a continuación, los dispositivos se comportan de la misma manera que el ejemplo de la figura 2.16.

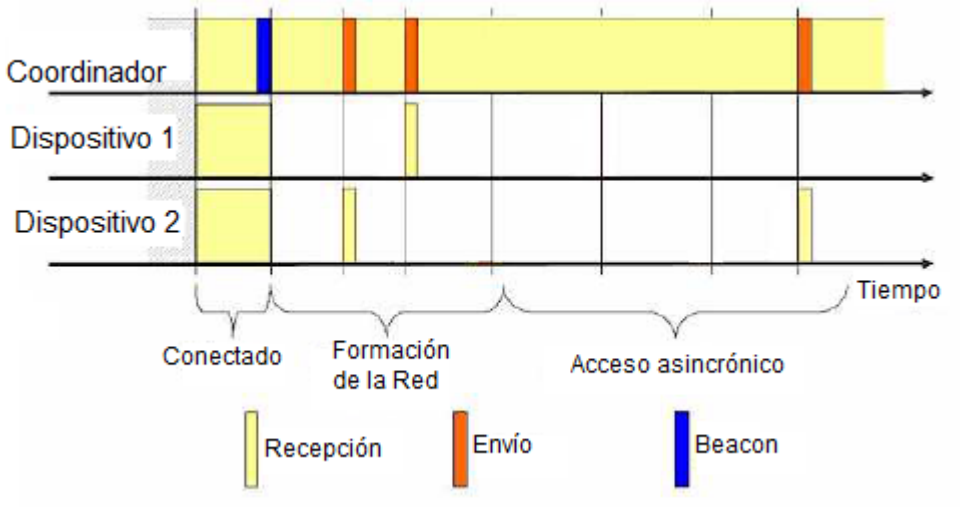


Figura 2. 17: Representación de una red sin beacon.
Fuente: (Kaushal et al., 2014)

2.9.3. La Capa de Red

Esta capa comprende además de la información de transporte en redes $ZigBee$ también soportar las aplicaciones de estos dispositivos. Para desempeñar este papel, se le han concedido algunas características descritas como:

- Scan de red: La capacidad de un dispositivo para detectar uno o más canales activos en su alcance de comunicación.
- Crear / unirse a PAN: Crear una red local y unirse a una ya existente.
- Detección de dispositivos: Capacidad para encontrar dispositivos en el canal activo en el PAN.
- Descubrimiento de Servicio: El descubrimiento de un servicio y la capacidad de determinar qué servicios admite los dispositivos dentro de una red.

- Encuadernación: Capacidad de comunicación sin nivel de aplicación con otro dispositivo de red.

2.10. Características de ZigBee.

2.10.1. Número de canales y frecuencias

La norma IEEE 802.15.4 regula 27 canales de frecuencia libres para la operación del ZigBee, tales canales se dividen de acuerdo con la onda portadora generada por el módulo transceptor y se dividen en tres bandas de frecuencia. La primera va de 868MHz hasta 868,6MHz, soporta sólo un canal y se utiliza sólo en Europa (ver la figura 2.18 a).

La segunda pista comienza en 902MHz y termina en 928MHz, ofrece 10 canales y se utiliza comúnmente en América del Norte (ver la figura 2.18 b). Por último, la última pista va de 2,4GHz hasta 2,4845GHz, ofrece 16 canales y se utiliza en todo el mundo (ver figura 2.18 c). La tabla 2.3 muestra cómo calcular el rango de frecuencia central de cada canal.

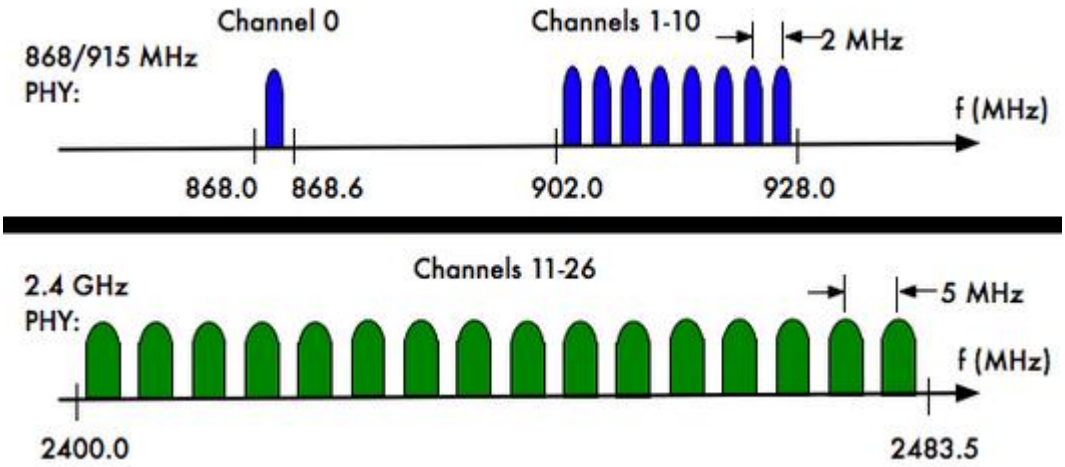


Figura 2. 18: Estructura de canales IEEE 802.15.4
Fuente: (Marques, 2017)

Tabla 2. 3: Frecuencia central de los canales

Número de canal	Frecuencia central del canal (MHz)
K = 0	868,3
K = 1, 2, …, 10	906 + 2 (K-1)
K = 11, 12, …, 26	2405 (K-11)

Fuente: (Marques, 2017)

2.10.2. Modulación

La modulación de las señales en redes ZigBee se lleva a cabo de dos formas diferentes, dependiendo del tipo de capa física usada. Para las capas físicas de 868/915 MHz la modulación es del tipo BPSK (Binary Phase Shift Keying) ya para las de 2,4 GHz la modulación utilizada es la OQPSK (Offset Quadrature Phase Shift Keying).

La modulación BPSK funciona de acuerdo con la figura 2.19, donde se muestran tres señales diferentes. El primero de ellos se llama señal modulante, es la información propiamente dicha que debe enviarse de un dispositivo a otro en la red, se trata de una secuencia de bits que traducen los datos de sensores u otros dispositivos conectados a los transceptores ZigBee.

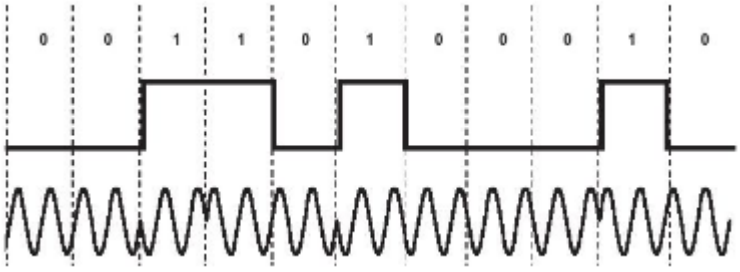


Figura 2. 19: Esquema de modulación BPSK
Fuente: (Sushmaja & Noorbasha, 2013)

La segunda señal es la onda portadora analógica, en el caso del ZigBee se trata de un signo senoidal en las frecuencias de 868/915 MHz o 2,4GHz, es a través de su deformación que se generará la señal modulada. La tercera señal se llama la portadora modulada, se transmite eficazmente desde un transceptor a otro de la red. Cada vez que la señal de modulación cambia el estado de un bit (0 a 1 o 1 a 0) la portadora analógica se somete a una inversión en la capa 180, haciendo por ello que la portadora modulada. De esta forma es posible reconstruir los datos que estaban en el transmisor de radio en el receptor por las técnicas de demodulación en fase.

En la figura 2.20 se expone gráficamente O-QPSK modulación que funciona de una manera similar a la BPSK. La señal modulante se agrupa en conjuntos de dos bits (a y b), denominados DBITS, en cada evento donde uno de estos pares se identifica la señal modulada sufre una deformación predefinida, según la tabla 2.4.

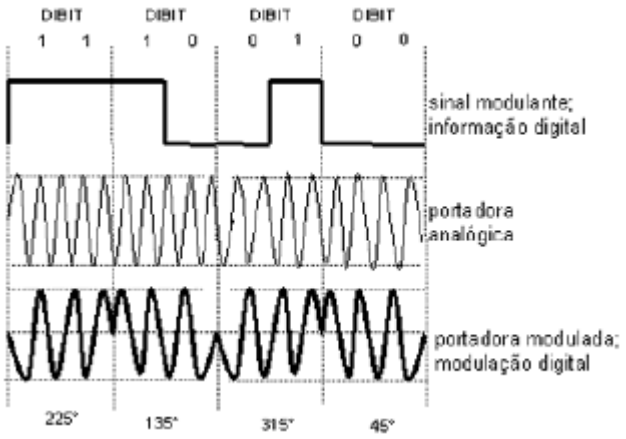


Figura 2. 20: Esquema de modulación O-QPSK
Fuente: (Sushmaja & Noorbasha, 2013)

Tabla 2. 4: Ángulo de deformación de fase en la modulación O-QPSK

Bit a	Bit b	Desfase (º)
0	0	45
0	1	315
1	0	135
1	1	225

Fuente: (Sushmaja & Noorbasha, 2013)

2.10.3. Sensibilidad y Potencia

La especificación para la sensibilidad del estándar ZigBee regula -85 dBm para la capa física de 2,4GHz y -92 dBm para las capas de 868 / 915MHz. La potencia también varía de acuerdo a la capa física utilizada, pero el estándar regula el mínimo 1 mW por dispositivo capaz de cubrir un área en el interior de 10 m a 20 m y un área al aire libre hasta 100 m. Los dispositivos XBee-PRO™ son modificadas para lograr un mejor rendimiento y tienen una sensibilidad de -100 dBm y 100 mW de potencia que les da una autonomía teórica de 100 a 200 m en interiores y exteriores de hasta 1,6 km.

2.10.4. Interferencia

Los transceptores que operan a 2,4 GHz sufren de interferencias generadas por otros dispositivos que operan en las pistas cercanas, como teléfonos y ordenadores Wi-Fi. Sin embargo, el estándar IEEE 802.15.4 ofrece este tipo de fallo cuando se permite que la baja calidad de servicio y no requiere comunicación síncrona entre dispositivos.

2.10.5. Seguridad

En las redes ZigBee, la capa MAC utiliza el estándar AES (Advanced Encryption Standard) proporcionar un algoritmo de 128 bits para cifrar los datos. Aunque este procesamiento algoritmo para ser realizada por la capa MAC, las capas superiores son el enlace en él que controlan nivel es para ser utilizado, puede ser: no seguridad; el control de acceso a los datos y simétricas de 128 bits AES clave.

2.11. Comparación con otras tecnologías inalámbricas

En informática, hay dos tecnologías inalámbricas que son dignas de mención en comparación con $ZigBee$, que son Bluetooth (IEEE 802.15.1) y Wi-Fi (IEEE 802.11). Wi-Fi por ser ampliamente utilizado en redes residenciales e incluso en algunas aplicaciones integradas y el Bluetooth por pertenecer a la misma categoría que el $ZigBee$ de dispositivos PAN.

En términos de aplicación el Bluetooth se destaca en funciones que requieren media tasa de transferencia de datos, a diferencia del $ZigBee$ que fue creado para actividades de baja tasa de transferencia y poco consumo de energía. Bluetooth se utiliza básicamente para interconectar dispositivos electrónicos sin necesidad de usar cables. Esta actividad requiere una conexión constante entre los dispositivos aumentando así el consumo de energía necesario para crear y mantener una red.

Por otro lado, $ZigBee$ proporciona la opción de mantener el equipo en un estado latente momentáneamente reducir casi a cero el consumo de energía de una red basada en ella. Wi-Fi es un estándar utilizado para la transferencia masiva de datos en redes locales. Fue desarrollado para reemplazar los cables convencionales en aplicaciones residenciales e industriales. Además de un alto rendimiento, alto consumo de energía y los altos costos son algunas de las características que distinguen a la ZigBee. La tabla 2.5 hace un comparativo más detallado entre las tecnologías descritas.

Tabla 2. 5: Comparación entre tecnologías inalámbricas

Características	Wi-Fi (WLAN)	Bluetooth (WLAN/WPAN)	ZigBee (WPAN)
Estándar	802.11	802.15.1	802.15.4
Corriente de transmisión	400 mA	40 mA	35 mA
Consumo de energía	20 mAh	200 µAh	3 µAh
Complejidad	Complejo	Muy complejo	Simple
Por Maestro	32	7	65535
Alcance	100m	10m	100m
Extensible	Posibilidad de roaming	No, no	Sí
Tasa de transferencia	11 a 54 Mbps	1 Mbps	250 Kbps
Seguridad	Servicio de autenticación de identidad (SSID)	64bits, 128bits	128 bits AES y nivel de aplicación de usuario
Aplicación	Internet, Vídeo, E-mail	Sustitución de cables	Monitoreo y Control
Atributos	Confiabilidad	Conveniencia de Costo	Velocidad y flexibilidad

Elaborado por Attor

CAPÍTULO 3: Simulación de ZigBee.

3.1. Introducción.

Para el presente capítulo se desarrolla la simulación y evaluación de ZigBee en WSN, usando la herramienta de simulación GUI de MatLab. Las simulaciones remiten el modelamiento de una red WSN/Zigbee a través de varios escenarios, estos dependen del número de routers, número de dispositivos finales (sensores) y dos factores que dependen de la topología utilizada. La simulación realizada está basada en el GUIDE de (Koubaa, Alves, & Tovar, 2006).

3.2. Especificaciones de los escenarios de simulación para ZigBee en WSNs.

Para esta sección se especifican tres pruebas para el escenario de simulación que se modela en MatLab/Simulink. Las tres pruebas se describen en la sección 3.3, mientras que en las secciones 3.2.1 y 3.2.2 se especifican los modos beacon (baliza) y el acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA).

3.2.1. Modo Beacon.

Beacon es un pequeño dispositivo muy utilizado en comunicaciones inalámbricas, tales como: Bluetooth y ZigBee. Este tipo de red son organizadas empleando la topología en árbol, tanto para routers (enrutadores) y nodos coordinadores. Estos difunden señales beacons periódicamente para

intercambiar datos con sus "routers". Los "routers" monitorean las señales beacons del "nodo coordinador" para mantener la sincronización temporal e intercambiar datos con él. Con varios routers en la red, es probable que haya transmisión simultánea de señales de beacons, que pueden chocar unos con otros o con tramas de datos, causando pérdida de sincronización en la red. Este problema de pérdida de sincronismo entre nodo coordinador y router puede resolverse de varias maneras.

En uno de los modos, el router debe evitar la transmisión de señal beacon al mismo tiempo que sus nodos vecinos o el período activo de supertrama de uno de ellos. Así, los routers vecinos deben intercalar sus períodos activos de supertrama. Por ejemplo, digamos que un nuevo router comenzó a participar en una red. En primer lugar, se debe determinar el momento en que ocurren los beacons y la supertrama de los períodos activos de sus nodos vecinos.

El enrutador deberá, a partir de entonces, transmitir sus señales beacon sin un momento en que no esté ocurriendo ningún otro período activo de sus nodos vecinos. A la vista de esto, los routers sólo necesitan precalentarse con el período activo de sus nodos vecinos y no de todos los routers de la red. Por lo tanto, se permite la superposición de períodos activos entre enrutadores no vecinos.

Un segundo modo, más fácil y directo, es evitar la superposición de los períodos activos entre cualesquiera pares de enrutadores de la red, independientemente de si son vecinos o no, e incluso si una superposición no lleva a una colisión de beacons. Este método es muy seguro, pero no es viable cuando hay un gran número de routers, ya que el intervalo de tiempo reservado para cada período activo sería muy pequeño. En la figura 3.1 se muestra el funcionamiento de este esquema.

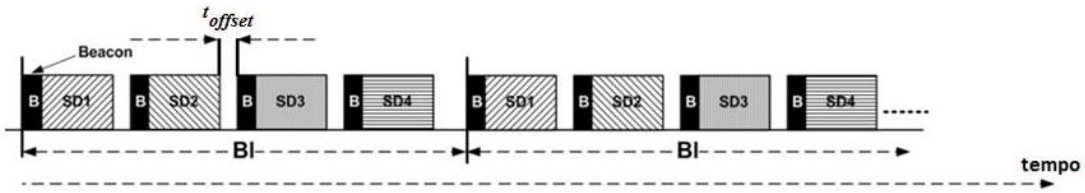


Figura 3. 1: Enfoque de programación Beacon en ZigBee.
Fuente: (Koubaa et al., 2006)

En el enfoque de programación Beacon, las señales se inician en secuencia. Una vez finalizado el primer período activo, un segundo enrutador transmite una señal beacon, y después del final del segundo período activo, un tercer enrutador transmite la señal beacon, y así sucesivamente. Para que esta secuencia funcione en una red con enrutadores, todos ellos con los mismos valores de orden de supertramas *(Superframe Order; SO)*, y orden de Beacon *(Beacon Order, BO)*, la siguiente afirmación debe ser verdadera:

$$BI \geq N \cdot SD$$

Donde, BI, es el intervalo Beacon y SD, es la duración de supertrama. Por ejemplo, los routers que utilicen transceptores de 2.4 GHz operan con 1

símbolo equivalente a 16 us. Por lo tanto, para una red ZigBee $BI > N \cdot SD$ las señales Beacon son separadas $SD + T_{offset}$ tal como la figura 3.1.

3.2.2. Acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA).

Para el estándar IEEE 802.15.4, la capa MAC está basado en contención ya sea ranurada o CSMA/CA sin ranuras, dependiendo del comportamiento de funcionamiento de la red: modos habilitados para beacon o no habilitados para beacon, respectivamente. El mecanismo CSMA/CA se basa en períodos de Backoff o retroceso (con duración de 20 símbolos). Se utilizan tres variables para programar el acceso al medio:

a. Número de Backoffs *(Number of Backoffs, NB)*: representa el número de intentos fallidos de acceso al medio.
b. Ventana de contención *(Contention Window, CW)*: representa el número de períodos de retroceso que deben estar claros antes de iniciar la transmisión.
c. Exponente de Backoff *(Backoff Exponent, BE)*: permite calcular el número de backoffs de espera antes de intentar acceder al medio nuevamente.

Para este escenario, los dispositivos de función completa *(Full Function Device, FFD)* del estándar IEEE 802.15.4 tienen tres modos de operación diferentes, que son:

a. El nodo coordinador de red de área personal *(Personal Area Network, PAN)*: este dispositivo identifica su propia red, así como sus configuraciones, a las que pueden estar asociados otros dispositivos. En ZigBee, este dispositivo se conoce como ZigBee Coordinator (ZC).
b. El coordinador: proporciona servicios de sincronización a través de la transmisión de beacons. Este dispositivo debe estar asociado a un coordinador PAN y no crea su propia red. En ZigBee, este dispositivo se conoce como ZigBee Router (ZR).
c. El dispositivo final: un dispositivo que no implementa las funcionalidades anteriores y debe asociarse con un ZC o ZR antes de interactuar con la red. En ZigBee, este dispositivo se denomina ZigBee End Device (ZED).

El dispositivo de función reducida *(Reduced Function Device, RFD)* es un dispositivo final que funciona con la implementación del estándar IEEE 802.15.4. Un RFD está destinado a aplicaciones que son extremadamente simples, tales como un interruptor de luz o un sensor pasivo de infrarrojos; No tienen la necesidad de enviar grandes cantidades de datos y sólo pueden asociarse con un único FFD a la vez.

A lo largo del desarrollo de simulación del presente trabajo de titulación, los modos operativos de IEEE 802.14.5 y los nombres de los dispositivos ZigBee se utilizan indistintamente como ZC=ZigBee Coordinador, ZR=ZigBee Router y ZD= ZigBee End Device).

3.3. Escenario de simulación de la tecnología ZigBee en WSNs.

En esta sección se desarrolla el escenario de simulación ZigBee conocido como el estándar IEEE 802.15.4 empleando topología de árbol que utiliza modo Beacon y que con ayuda de información de la página **www.open-zb.net.** Para esto fue necesario implementar una interfaz gráfica de usuario, también conocida como GUI de MatLab. Para iniciar con el desarrollo del GUI es necesario abrir la interfaz tal como se muestra en la figura 3.2.

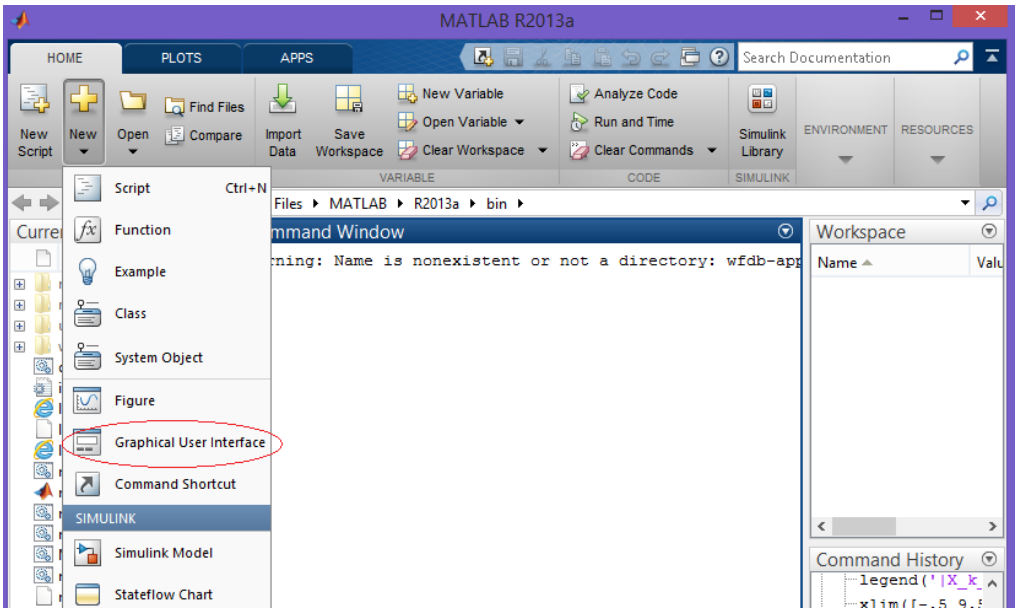


Figura 3. 2: Procedimiento para abrir la plataforma de interfaz gráfica de usuario (GUI) de MatLab.
Elaborado por: Autora

Posterior, en la figura 3.3 se muestra la ventana del GUIDE Quick Start, donde se llama a los GUIDE Templates. Para lo cual es necesario crear un Blank GUI. Mientras que las herramientas de GUI están disponibles en el editor de diseño *(Layout Editor)* tal como se muestra en la figura 3.4.

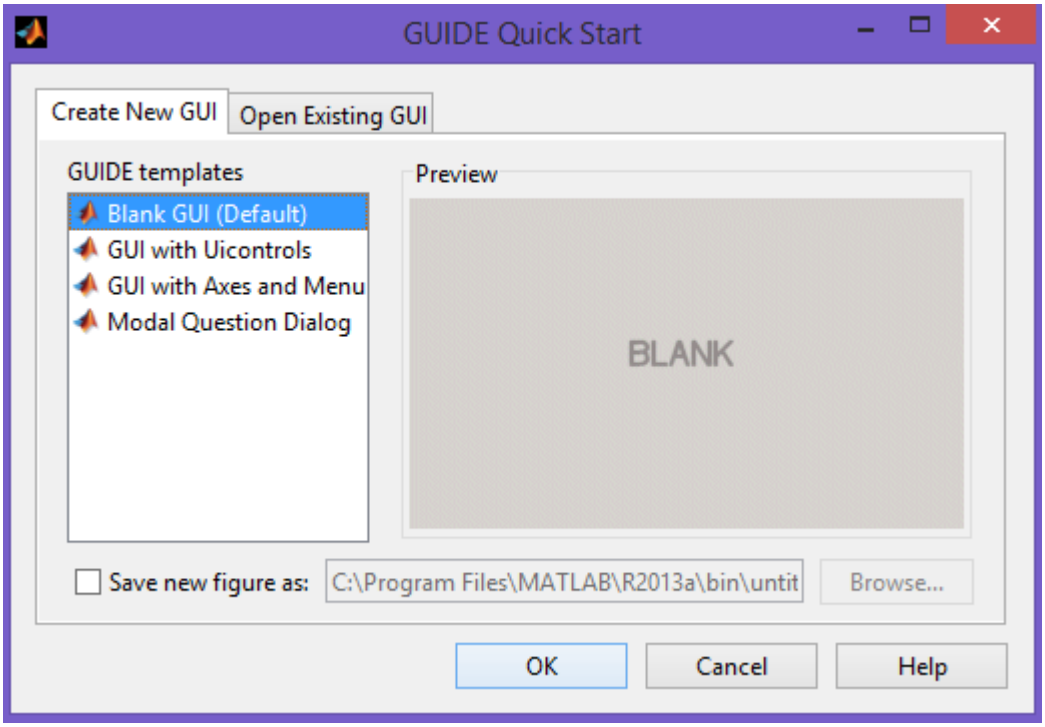


Figura 3. 3: Ventana de creación de nuevo diseño de GUI.
Elaborado por: Autor

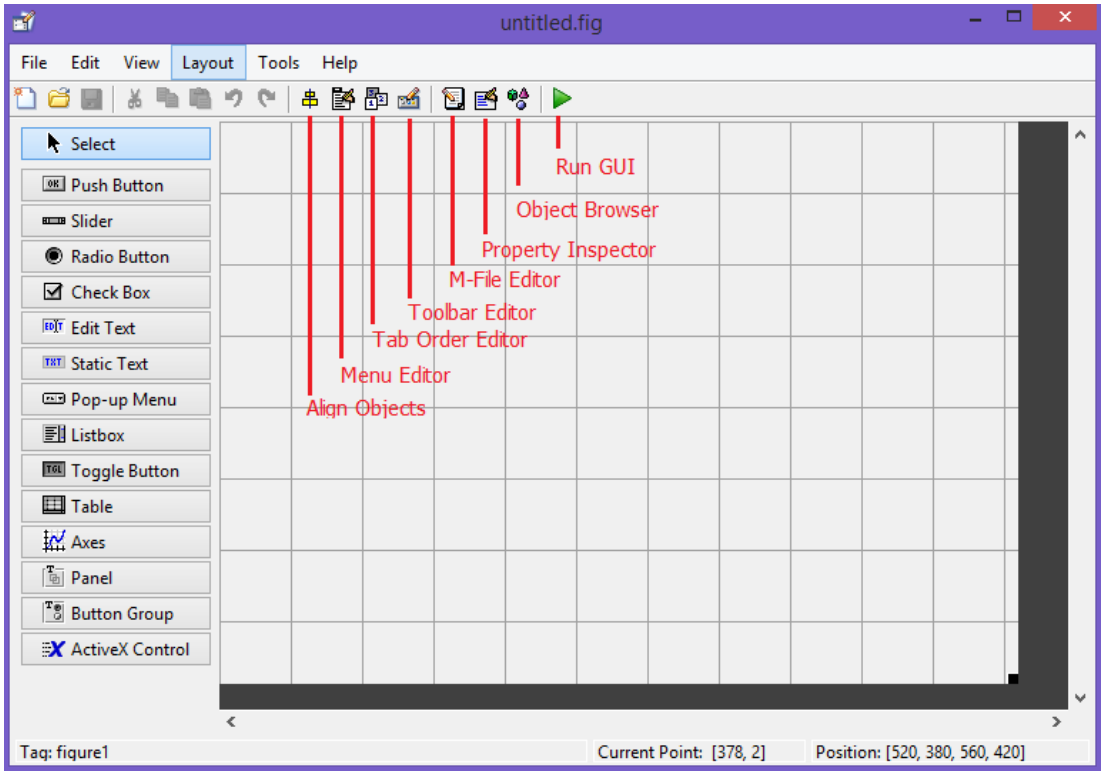


Figura 3. 4: Barra de herramientas de la interfaz gráfica de usuario (GUI).
Elaborado por: Autor

En la figura 3.5 se muestra la interfaz desarrollada en GUI de MatLab, donde se escriben los parámetros de entrada: (a) especificación de topología en árbol, (b) tráfico basado en sensores, y (c) del estándar IEEE 802.15.4.

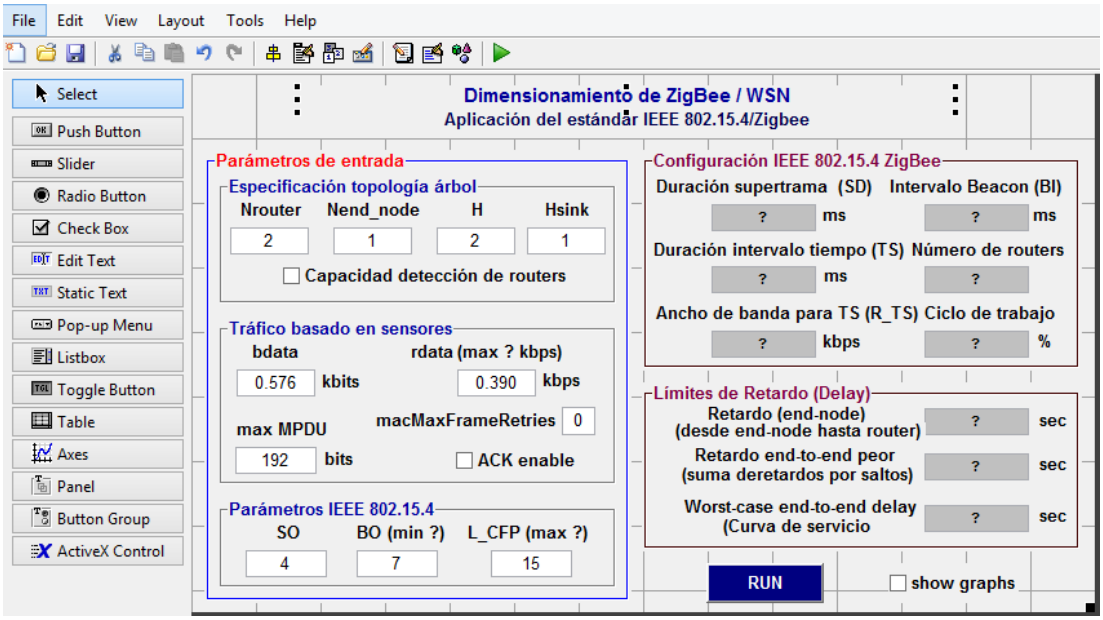


Figura 3. 5: Interfaz gráfica de usuario para escenario de simulación 1.
Elaborado por: Autor

Para modelar la tecnología ZigBee es necesario considerar los parámetros de entrada, que son:

1. Especificación de topología de árbol: en la figura 3.6 se muestra los parámetros que se describen de la siguiente manera:

   (a) Nrouter: número máximo de routers asociados a un router principal,

   (b) Nend_node: número máximo de nodos final asociados a un router principal, es decir, la simulación considera que los end-node sean dispositivos finales y que poseen sensores de medición,

   (c) H: altura máxima de la red que corresponde al nodo coordinador,

(d) Hsink: profundidad del router que alberga el dispositivo receptor, el mismo es autónomo y móvil de la red que se encarga de recoger los datos medidos por los nodos sensores (end_node), **(e)** capacidad de detección de routers: siempre que los routers tengan incorporados sensores se comportan con capacidad de detección, de lo contrario, sólo sirve como transmisor de mediciones realizadas por end_node,

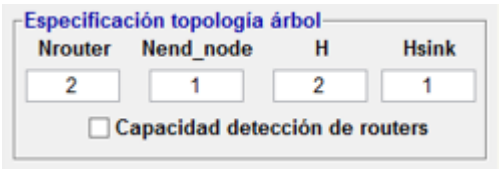


Figura 3. 6: Parámetros de especificación de la topología en árbol.
Elaborado por: Autor

2. Tráfico basado en sensores: en la figura 3.7 se muestra los parámetros y que son descritos de la siguiente manera:

(a) bdata: es el tamaño de ráfaga (burst) máximo del flujo de datos,

(a) rdata: velocidad de transferencia promedio de las mediciones de los sensores que viene de los end_node,

(b) maxMPDU: tamaño máximo de tramas en la MAC por el usuario,

(c) macMax: que sería el número de reintentos de tramas,

(d) ACK enable: habilitar al dispositivo para acuse de recibo de mensajes por cada paquete de datos recibidos.

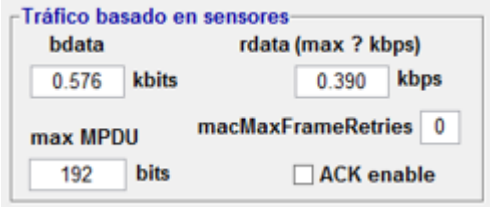


Figura 3. 7: Parámetros del tráfico basado en sensores inalámbricos.
Elaborado por: Autor

3. Especificación del estándar IEEE 802.15.4: en la figura 3.8 se muestra los parámetros y que son descritos de la siguiente manera:

(a) BO: es el orden de baliza (beacon) o exponente que se utiliza para obtener el período de supertrama,

(b) SO: es el orden de supertrama o exponente que se utiliza para obtener el período activo de la supertrama,

(c) L_CFP: número de slots reservados en la parte del período libre de contención *(Contention Free Period, CFP)* durante el período activo de las supertramas. El período activo de la supertrama se subdivide en 16 ranuras con el mismo tamaño. La especificación IEEE 802.15.4 relata que al menos una ranura se debe dejar para el período de acceso de contención *(Contention Access Period, CAP)*, aunque reservar sólo una ranura no es viable en la práctica.

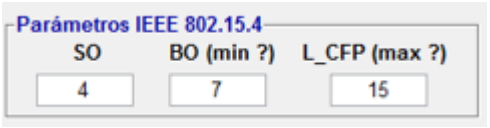


Figura 3. 8: Parámetros del estándar IEEE 802.15.4.
Elaborado por: Autor

De acuerdo al trabajo de Koubaa et al., (2006), el BI y SD que se muestran en la figura 3.5 son determinados por los parámetros SO y BO, de acuerdo a la siguiente ecuación:

$$\left.\begin{aligned} BI &= aBaseSuperframeDuration \cdot 2^{BO} \cdot 16\mu s \\ SD &= aBaseSuperframeDuration \cdot 2^{SO} \cdot 16\mu s \end{aligned}\right\} para\ 0 \leq SO \leq BO \leq 14$$

3.4. Resultados obtenidos del escenario de simulación de tecnología ZigBee en WSNs.

En la tabla 3.1 se indican los valores paramétricos del modelado para el primer escenario de simulación.

Tabla 3. 1: Configuración de los parámetros de entrada.

Datos	Prueba 1	Prueba 2	Prueba 3
Nrouter	1	3	1
Nend_node	3	1	1
H	1	1	3
Hsink	0	0	0
Bdata	0 kbits	0 kbits	0 kbits
Rdata	1 kbps	1 kbps	1 kbps
maxMPDU	1016 bits	1016 bits	1016 bits
SO	6	6	8
BO (mín)	8	10	10
L_CFP (máx)	8	12	15

Elaborado por: Autor

Para la primera prueba (ver tabla 3.1) se procede a obtener los valores teóricos de los parámetros: intervalo Beacon (BI), Duración Supertrama (SD), Duración intervalo de tiempo (TS) y Ciclo de trabajo. En la figura 3.9 se puede observar el resultado obtenido después de ejecutar la simulación prueba 1.

$$BI = 960 \cdot 2^8 \cdot 16\mu s = 3932{,}16\ ms$$

$$SD = 960 \cdot 2^6 \cdot 16\mu s = 983{,}04\ ms$$

$$TS = \frac{960 \cdot 2^{SO}}{16} \cdot 16\mu s = \frac{960 \cdot 2^6}{16} \cdot 16\mu s = 61{,}44\ ms$$

$$Ciclo = \frac{SD}{BI} = \frac{2^{SO}}{2^{BO}} \cdot 100 = \frac{2^6}{2^8} \cdot 100 = 25\%$$

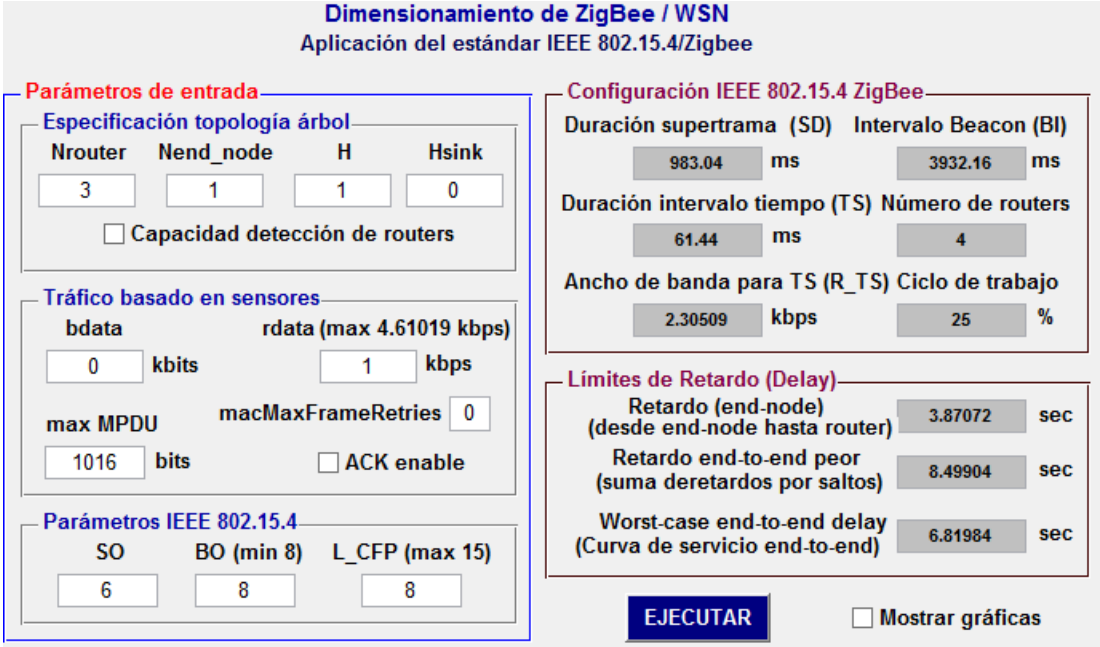


Figura 3. 9: Resultado obtenido de simulación ZigBee para la prueba 1.
Elaborado por: Autor

La segunda prueba (ver tabla 3.1) también se obtienen los valores teóricos de los parámetros: intervalo Beacon (BI), Duración Supertrama (SD), Duración intervalo de tiempo (TS) y Ciclo de trabajo. En la figura 3.10 se puede observar el resultado obtenido después de ejecutar la simulación prueba 2.

$$BI = 960 \cdot 2^{10} \cdot 16\mu s = 15728{,}6\ ms$$

$$SD = 960 \cdot 2^{6} \cdot 16\mu s = 983{,}04\ ms$$

$$TS = \frac{960 \cdot 2^{SO}}{4} \cdot 16\mu s = \frac{960 \cdot 2^{6}}{4} \cdot 16\mu s = 61{,}44\ ms$$

$$Ciclo = \frac{SD}{BI} = \frac{2^{SO}}{2^{BO}} \cdot 100 = \frac{2^{6}}{2^{10}} \cdot 100 = 6.25\%$$

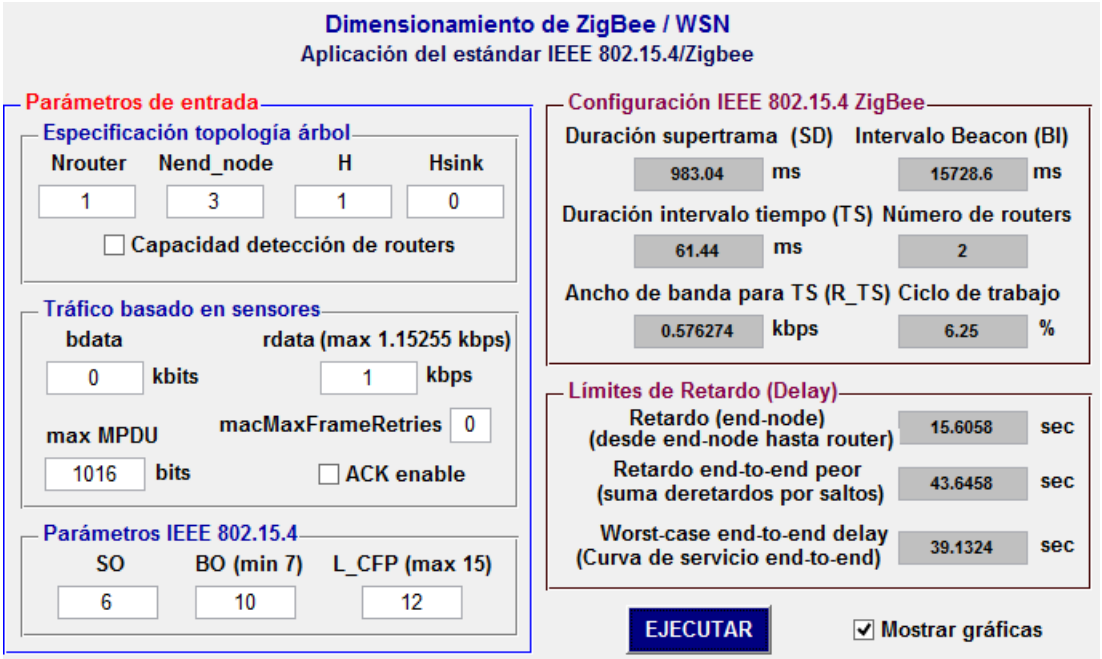


Figura 3. 10: Resultado obtenido de simulación ZigBee para la prueba 2.
Elaborado por: Autor

Finalmente, en la tercera prueba (ver tabla 3.1) se procede a obtener los valores teóricos de los parámetros: intervalo Beacon (BI), Duración Supertrama (SD), Duración intervalo de tiempo (TS) y Ciclo de trabajo. En la figura 3.11 se puede observar el resultado obtenido después de ejecutar la simulación prueba 3.

$$BI = 960 \cdot 2^{10} \cdot 16\mu s = 15728{,}6\ ms$$

$$SD = 960 \cdot 2^{6} \cdot 16\mu s = 983{,}04\ ms$$

$$TS = \frac{960 \cdot 2^{SO}}{4} \cdot 16\mu s = \frac{960 \cdot 2^{8}}{4} \cdot 16\mu s = 61{,}44\ ms$$

$$Ciclo = \frac{SD}{BI} = \frac{2^{SO}}{2^{BO}} \cdot 100 = \frac{2^{6}}{2^{8}} \cdot 100 = 25\%$$

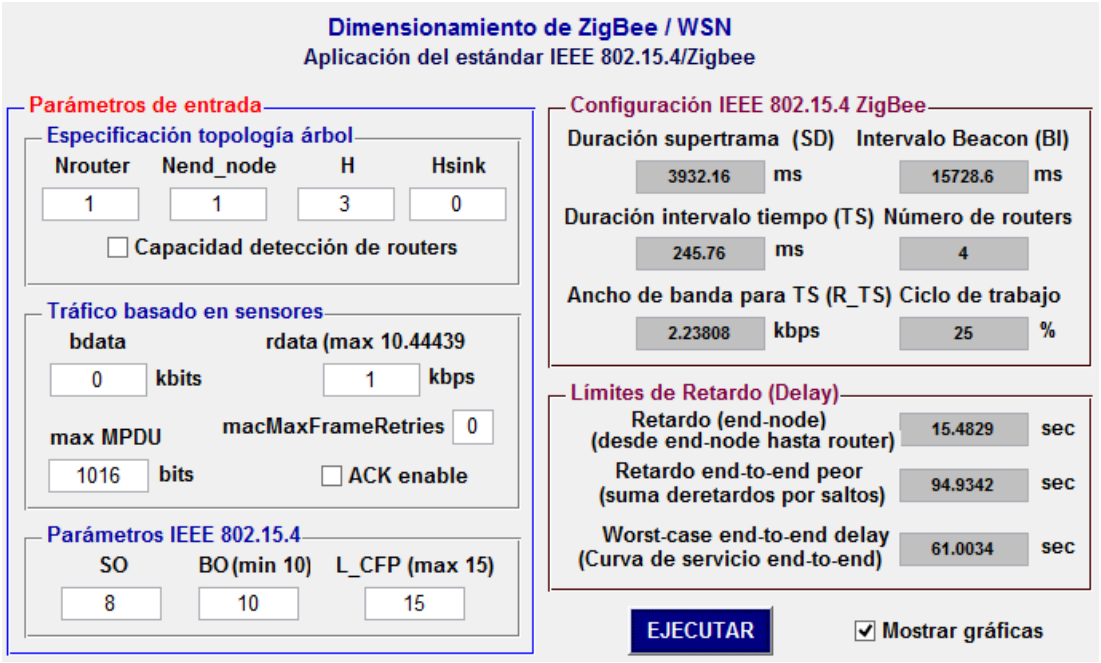


Figura 3. 11: Resultado obtenido de simulación ZigBee para la prueba 3.
Elaborado por: Autor

Finalmente, con todos los datos de las pruebas 1, 2 y 3 mostrados en la tabla 3.1 se pueden generar las gráficas de cada una de pruebas. Las figuras 3.12, 3.13 y 3.14 muestran los valores que se obtienen al ejecutar el modelado de ZigBee que guardan similitud a lo indicado en el estándar IEEE 802.14.5. Cada gráfico presenta tres agrupaciones. Para las figuras 3.12, 3.13 y 3.14, muestran en la primera agrupación el requisito de banda ancha (upstream) necesario para el enrutador. La segunda agrupación muestra el mínimo buffer necesario para el nodo coordinador. Y el tercer grupo muestra que el tiempo de retardo de la medición del sensor hasta llegar al punto dispositivo receptor. Los datos del (los) end-node (s) más alejado del receptor serán los que tomaron más tiempo para ser recibido por el receptor. Este tiempo de retardo más largo se calculará a partir del (los) end-node (s) más alejado del receptor.

En los tres escenarios, el (los) end-node (s) más alejado será aquel localizado en la mayor profundidad (depth) de la red.

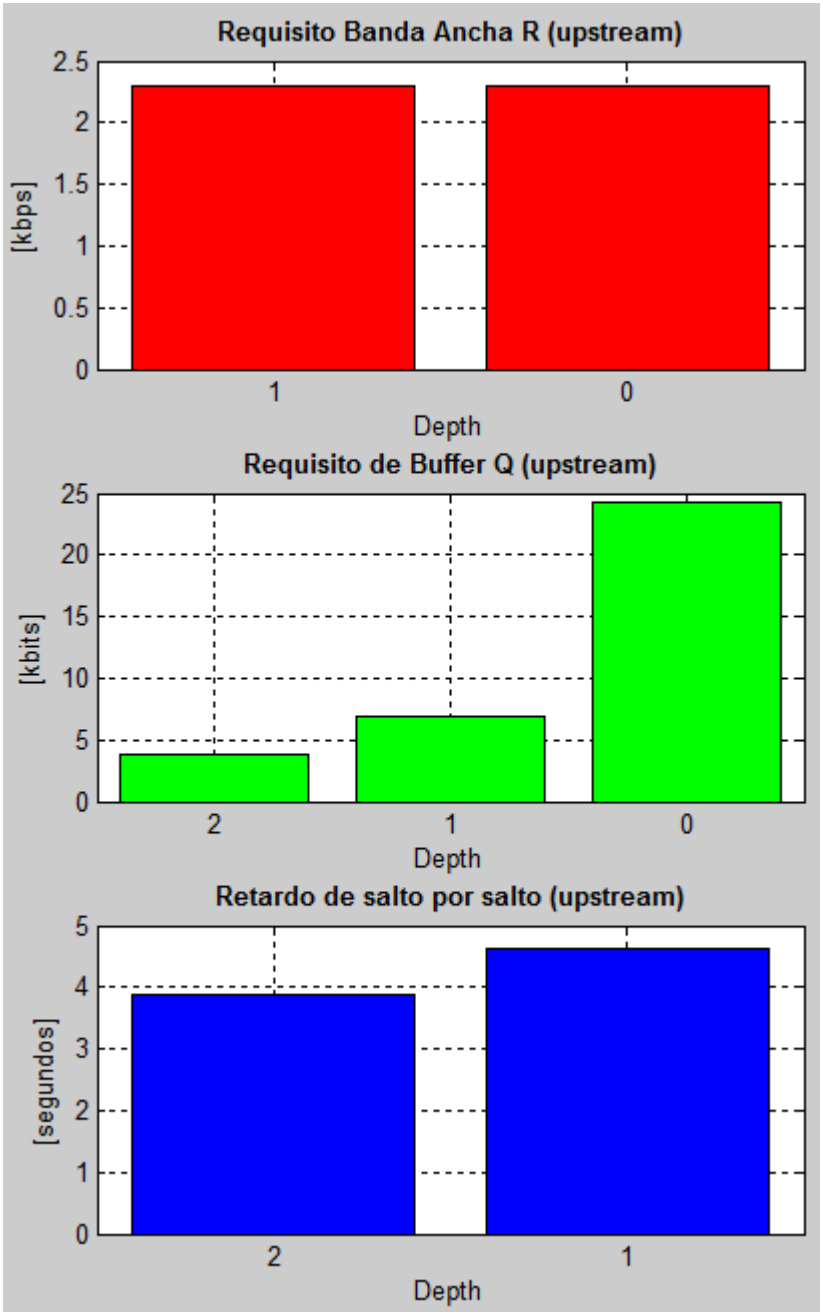


Figura 3. 12: Gráficas obtenida de la simulación ZigBee para la prueba 1.
Elaborado por: Autor

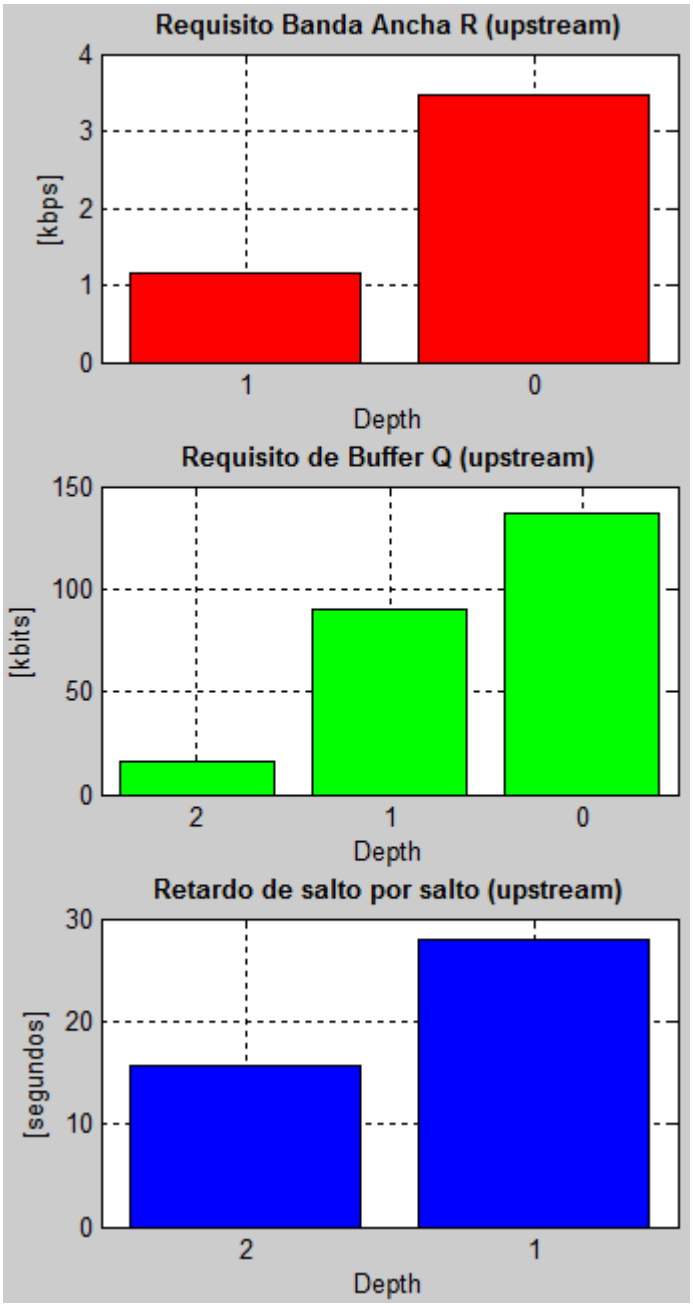


Figura 3. 13: Gráficas obtenida de la simulación ZigBee para la prueba 2.
Elaborado por: Autor

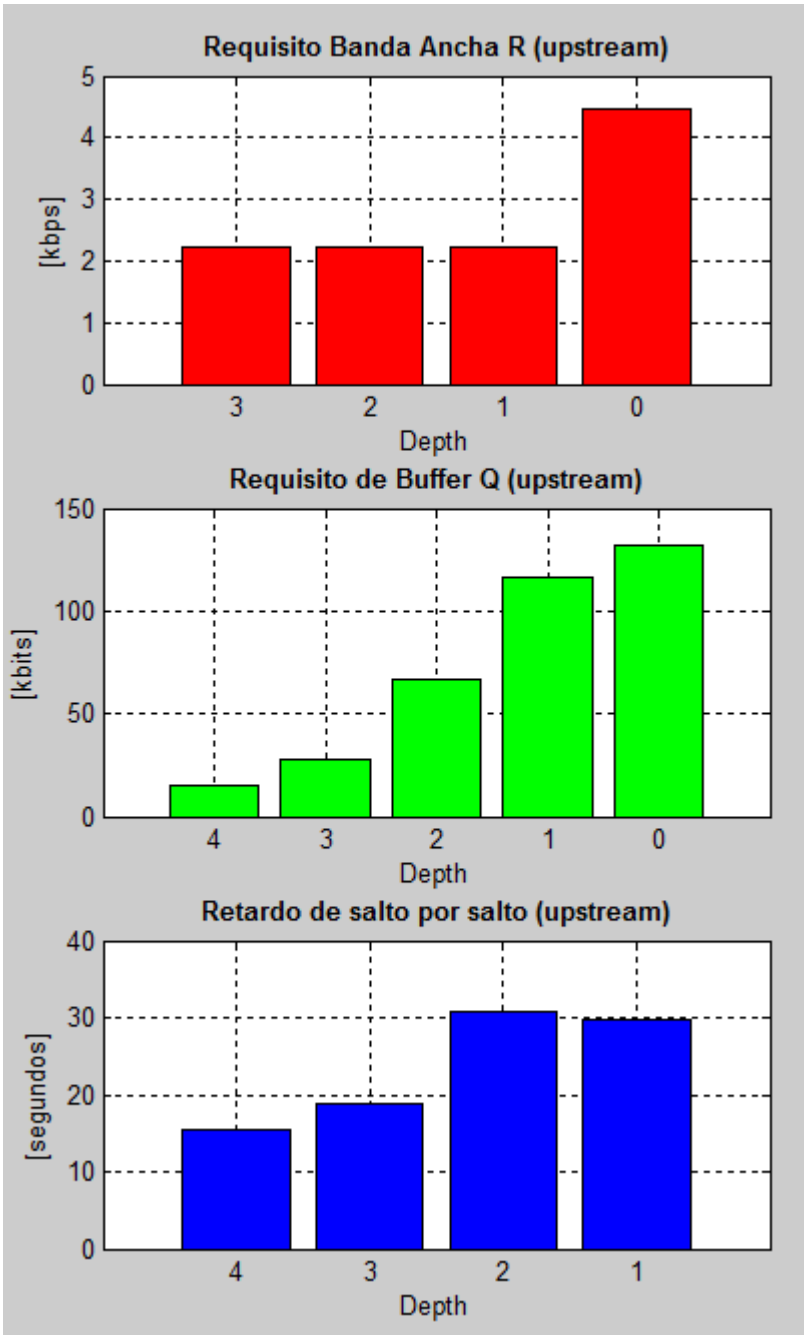


Figura 3. 14: Gráficas obtenida de la simulación ZigBee para la prueba 3.
Elaborado por: Autor

CAPÍTULO 4: Conclusiones y Recomendaciones.

4.1. Conclusiones

Sabiendo la relevancia de Zigbee en el escenario de estándares inalámbricos, este trabajo abordó una variedad de temas relacionados con su arquitectura de protocolos, haciendo un retrato de las funciones y características principales de Zigbee. Antes de describir la pila de protocolos, el trabajo contextualizó el Zigbee dentro del universo de redes inalámbricas, proporcionando conceptos generales sobre redes inalámbricas, redes de sensores inalámbricas (WSN) y aplicaciones para Zigbee.

Las tecnologías de redes y dispositivos inalámbricos tienen un futuro prometedor en varias áreas, por ser visualmente limpias, por la movilidad alcanzada y por eliminar los "desagradables" cables. Una de estas áreas prometedoras es la de sensorización remota, en la que el Zigbee y el estándar IEEE 802.15.4 son protocolos destacados, por cubrir muchos de los requisitos exigidos: bajo consumo alcanzado con eficiencia energética; redes dinámicas y flexibles; y simplicidad de protocolos en dispositivos con memoria limitada.

Finalmente, las pruebas realizadas del estado de la técnica utilizada en el trabajo de titulación a través del modelo general de WSN mediante la topología de árbol de clúster y del dimensionamiento de los recursos de red fueron necesarios para el análisis correcto del rendimiento de tiempo.

4.2. Recomendaciones.

El modelado y la metodología utilizada en el presente proyecto orientan a proponer nuevos trabajos de titulación o de investigación. Por ejemplo, pueden desarrollar un modelado para mejorar la optimización del dimensionamiento de IEEE 802.15.4 / Zigbee.

Otro problema a resolver sería la optimización del mecanismo de programación de beacon para que los routers funciones a mayor profundidad (depth) cercanos al nodo coordinador, para que funcionen a un ciclo de servicio más alto que los enrutadores a profundidades más bajas.

A futuro se puede realizar el análisis en el dominio de la frecuencia y el esparcimiento espectral generado por transceptores con frecuencia de 2,4GHz en la codificación en chips.

Bibliografía

Cortés C., M., & Iglesias L., M. (2004). *Generalidades sobre Metodología de la Investigación* (Colección Material Didactico). Campeche, México: Universidad Autónoma del Carmen. Recuperado a partir de http://www.unacar.mx/contenido/gaceta/ediciones/metodologia_investigacion.pdf

Eiza, M. H., Ni, Q., Owens, T., & Min, G. (2013). Investigation of routing reliability of vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking*, *2013*(1). https://doi.org/10.1186/1687-1499-2013-179

Heinemann, A. (2007). *Collaboration in Opportunistic Networks*. Recuperado a partir de http://tuprints.ulb.tu-darmstadt.de/834/1/heinemann07-diss.pdf

Hwang, S., & Yu, D. (2012). Remote Monitoring and Controlling System based on ZigBee Networks. *International Journal of Software Engineering and Its Applications*, *6*(3), 35–42.

Kaushal, K., Kaur, T., & Kaur, J. (2014). ZigBee based Wireless Sensor Networks. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *5*(6), 7752–7755.

Khoukhi, L., Badis, H., Merghem-Boulahia, L., & Esseghir, M. (2013). Admission control in wireless ad hoc networks: a survey. *EURASIP Journal on Wireless Communications and Networking*, *2013*, 109. https://doi.org/10.1186/1687-1499-2013-109

Koubaa, A., Alves, M., & Tovar, E. (2006). Modeling and Worst-Case Dimensioning of Cluster-Tree Wireless Sensor Networks (pp. 412–421). IEEE. https://doi.org/10.1109/RTSS.2006.29

Lilien, L., Kamal, Z. H., Bhuse, V., & Gupta, A. (2007). The Concept of Opportunistic Networks and their Research Challenges in Privacy and Security. En S. K. Makki, P. Reiher, K. Makki, N. Pissinou, & S. Makki (Eds.), *Mobile and Wireless Network Security and Privacy* (pp. 85–117). Boston, MA: Springer US. Recuperado a partir de http://link.springer.com/10.1007/978-0-387-71058-7_5

Macom. (2016). Wireless Network Infrastructure. Recuperado el 15 de julio de 2017, a partir de https://www.macom.com/wirelessinfra

Marques, B. F. (2017). *Application-Driven Wireless Sensor Networks*. Unpublished. Recuperado a partir de http://rgdoi.net/10.13140/RG.2.2.25931.39202

Ouni, S., & Ayoub, Z. (2013). Predicting communication delay and energy consumption for IEEE 802.15.4/ZigBee Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC)*, *5*(1), 141–152.

Pathak, S., Kumar, M., Mohan, A., & Kumar, B. (2015). Energy Optimization of ZigBee Based WBAN for Patient Monitoring. *Procedia Computer Science*, *70*(Supplement C), 414–420. https://doi.org/10.1016/j.procs.2015.10.055

Ryaan, D. (2012, agosto 7). How To Enable Ad-Hoc Wi-Fi Detection for Android Phones. Recuperado el 15 de julio de 2017, a partir de https://ryaandavis.wordpress.com/2012/08/07/how-to-enable-ad-hoc-wi-fi-detection-for-android-phones/

Salazar Soler, J. (2016). *Redes inalámbricas*. European Virtual Learning Platform for Electrical and Information Engineering. Recuperado a partir de http://upcommons.upc.edu/handle/2117/100918

Seppänen, K., Kilpi, J., & Suihko, T. (2015). Integrating WMN Based Mobile Backhaul with SDN Control. *Mobile Networks and Applications*, *20*(1), 32–39. https://doi.org/10.1007/s11036-015-0574-7

Sharma, K., & Dhir, N. (2014). A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *5*(6), 7810–7813.

Somov, A., Baranov, A., & Spirjakin, D. (2014). A wireless sensor–actuator system for hazardous gases detection and control. *Sensors and Actuators A: Physical*, *210*, 157–164. https://doi.org/10.1016/j.sna.2014.02.025

Sushmaja, K., & Noorbasha, F. (2013). Implementation of Binary Shift Keying Techniques. *nternational Journal of Engineering Trends and Technology (IJETT)*, *4*(6), 2581–2583.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **CABEZAS CHALCO, GLORIA PIEDAD** con C.C: # 091579641-1 autor del Trabajo de Titulación: **Análisis y evaluación del protocolo ZigBee en aplicaciones de redes de sensores inalámbricos para comunicaciones P2P** previo a la obtención del título de **INGENIERA EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 15 de Septiembre de 2017

f. _____
Nombre: CABEZAS CHALCO, GLORIA PIIEDAD
C.C: 091579641-1

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	ANÁLISIS Y EVALUACIÓN DEL PROTOCOLO ZIGBEE EN APLICACIONES DE REDES DE SENSORES INALÁMBRICOS PARA COMUNICACIONES P2P		
AUTOR(ES)	CABEZAS CHALCO, GLORIA PIEDAD		
REVISOR(ES)/TUTOR(ES)	BOHÓRQUEZ ESCOBAR, CELSO BAYARDO		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	15 de Septiembre de 2017	**No. DE PÁGINAS:**	83
ÁREAS TEMÁTICAS:	Transmisiones, Comunicaciones Inalámbricas, Sistemas de Comunicación.		
PALABRAS CLAVES/ KEYWORDS:	COMUNICACIONES, INALÁMBRICAS, ZIGBEE, WSN, TOPOLOGÍAS, MATLAB.		

RESUMEN/ABSTRACT (150-250 palabras):

El desarrollo del trabajo de titulación consistió en realizar el análisis y evaluación de la tecnología ZigBee en aplicaciones de redes de sensores inalámbricos utilizando la comunicación P2P. Primero, se realiza las generalidades del trabajo, tales como, introducción, antecedentes, definición y justificación del problema a investigar, así como el objetivo general y objetivos específicos, hipótesis y metodología de investigación. Posterior, se describe los fundamentos teóricos de redes inalámbricas, redes oppnets (oportunistas) y ZigBee. En forma general, las redes inalámbricas son la mejor solución al momento de realizar transmisiones de datos de manera remota utilizando sensores para aplicaciones en comunicaciones punto a punto. Zigbee es una de las principales y más conocidas tecnologías de comunicación inalámbrica. Además de movilidad, característica típica de dispositivos inalámbricos, el Zigbee también posibilita dispositivos móviles de tamaño y peso reducido. Estas características, más el bajo consumo de energía alcanzado por dispositivos Zigbee, son esenciales en aplicaciones para las áreas de monitoreo remoto, control y sensoración, como por ejemplo para las redes WSN. Para poder realizar la parte final, se especifica los escenarios de simulación en Beacon y CSMA/CA. Finalmente, se desarrolla una interfaz gráfica (GUI) en MatLab que permitió modelar el comportamiento de la tecnología ZigBee mediante redes de sensores inalámbricos.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-9-82264923	E-mail: gpcabezas@gmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Córdova Rivadeneira Luis Silvio	
	Teléfono: +593-9-92305262	
	E-mail: luis.cordova@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
No. DE REGISTRO (en base a datos):	
No. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	