Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

Trabajo de Diploma

Propuesta de una Red Inalámbrica de Sensores para Edificios Docentes.

Autor: Antonio Pacheco Menéndez

Tutor: Dr. Félix Álvarez Paliza

Santa Clara

2015

“Año 57 de la Revolución”

Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

Trabajo de Diploma

Propuesta de una Red Inalámbrica de Sensores para Edificios Docentes.

Autor: Antonio Pacheco Menéndez

E-mail: apmenendez@uclv.edu.cu

Tutor: Dr. Félix Álvarez Paliza

Profesor Titular

Departamento de Telecomunicaciones y Electrónica

Facultad de Ingeniería Eléctrica

E-mail: fapaliza@uclv.edu.cu

Santa Clara

2015

"Año 57 de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de
Información Científico-Técnica

Pensamiento

"Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo."

Benjamin Franklin

Dedicatoria

A mis padres, por haber realizado innumerables hazañas por lograr mi felicidad.

Agradecimientos

A mis padres y abuelos, por su amor incondicional y eterno.

A mi hermana Dianita, ese diablillo menor que todos tenemos y que saca los mejor que llevamos dentro.

A mi novia y soñada esposa Mary, por su insuperable paciencia e incomparable cariño.

A mis amigos Roberto, Rigo, Hugo y Julio porque me han demostrado que aún existen personas de valor en este mundo.

A mi tutor por su valorable apoyo y su enseñanza rigurosa pero necesaria.

A mi laptop HP por ser una fiel maquinaria de guerra hasta el último momento.

A todos aquellos que de una forma u otra me han ayudado en cada paso que he dado por este camino de la vida.

Tarea Técnica

1. Evaluación de las arquitecturas (componentes de software y hardware) que presentan las Redes Inalámbricas de Sensores.
2. Selección del estándar de WSN a utilizar.
3. Analizar las aplicaciones de las redes WSN para edificios docentes.
4. Determinación de los sensores a utilizar en la aplicación tomando en cuenta el costo-beneficio.
5. Análisis de diferentes variantes de redes en cuanto a topologías, sensores, equipos, etc.
6. Evaluación del comportamiento o desempeño de la red para cada escenario.
7. Analizar los resultados.
8. Elaboración del informe del Trabajo de Diploma.

_____ _____

Firma del Autor Firma del Tutor

Resumen

El presenta Trabajo de Diploma se enfoca en el diseño y análisis de una propuesta de Red Inalámbrica de Sensores (WSN) para edificios docentes, pretendiéndose como resultado el dar solución a problemas reales existentes en la Universidad Central “Marta Abreu” de Las Villas como es el caso del hurto constante a sus medios materiales.

Para el diseño de esta red se ha tomado como referencia la arquitectura física de la Facultad de Ingeniería Eléctrica, implementado en ésta, una red de vigilancia utilizando sensores inalámbricos ZigBee y cámaras Wi-Fi operando dichos dispositivos en la banda de 2.4Ghz; además se hace uso de la herramienta de simulación OPNET Modeler 14.5 para analizar el desempeño de dicha red híbrida (ZigBee/Wi-Fi).

Palabras claves: Red Inalámbrica de Sensores, ZigBee, Wi-Fi, OPNET.

Tabla de contenidos

Pensamiento i
Dedicatoria ii
Agradecimientos iii
Tarea Técnica iv
Resumen v
Tabla de contenidos vi
Introducción 1
Capítulo I: Evaluación de las Redes Inalámbricas de Sensores 4
1. 1. Generalidades sobre las Redes Inalámbricas de Sensores 4
1. 2. Componentes de Hardware 5
1. 2. 1. Eficiencia energética 7
1. 3. Componentes de Software 8
1. 3. 1. Sistemas Operativos 9
1. 4. Estándares Inalámbricos 10
1. 4. 1. Estándar IEEE 802.11 11
1. 4. 2. Estándar IEEE 802.15.4 15
1. 4. 3. Estándar ZigBee 18
1. 5. Topologías de red 20
1. 5. 1. Formación de una red en estrella 21
1. 5. 2. Formación de una red punto a punto 21
1. 6. Estudio comparativo de Zigbee con otras tecnologías 22
1. 6. 1. Wi-Fi 23
1. 6. 2. Bluetooth 23
1. 6. 3. 6LoWPAN 24
1. 6. 4. WirelessHart 24
1. 6. 5. Z-wave 25
1. 6. 6. ULP Bluetooth 25
1. 7. Ejemplos de redes híbridas ZigBee/Wi-Fi 25

1. 7. 1. Monitoreo de Turbinas de viento generadoras de electricidad 26
1. 7. 2. Automatización del hogar 27
1. 8. Conclusiones del capítulo 29
Capítulo II: Procedimiento de Diseño de una WSN en un edificio docente.....30
2. 1. Selección de la banda de frecuencia.....30
2. 2. Coexistencia entre Wi-Fi y ZigBee.....30
2. 3. Caracterización de la red a diseñar.....32
2. 4. Selección del Hardware.....36
2. 5. Conclusiones del capítulo 38
Capítulo III: Análisis del Desempeño de la Red WSN.....39
3. 1. Herramienta OPNET Modeler 39
3. 2. Análisis del Escenario de la Facultad de Ingeniería Eléctrica 40
3. 2. 1. Arquitectura ZigBee.....41
3. 2. 2. Arquitectura WLAN.....43
3. 3. Análisis de los Resultados.....45
3. 3. 1. Resultados ZigBee 45
3. 3. 2. Resultados WLAN 46
3. 4. Conclusiones del capítulo 50
Conclusiones y Recomendaciones.....51
Conclusiones 51
Recomendaciones.....51
Referencias Bibliográficas.....52
Anexos 54
Anexo I: Tipos de sensores utilizados en Redes de Sensores Inalámbricas. 54
Anexo II: Hojas de Especificaciones de los dispositivos.....56
Anexo III: Resultados secundarios de la simulación. 61

Introducción

El mundo de las tecnologías constituye un campo de estudio y diseño en constante avance y movimiento, en permanente variación y evolución, que en la actualidad desarrolla cientos de equipos, que en muchos casos, difieren en gran medida de sus primeras versiones. La era tecnológica de este siglo se caracteriza sobre todo por la minimización, principalmente en lo referente a la electrónica, gracias al avance en materia de fabricación de componentes de baja potencia y económicos, con capacidad de detectar, procesar información y comunicarse con otros de forma inalámbrica. Gracias a la evolución en prestaciones y tamaño que nos ofrece la electrónica actual, disponemos de sensores capaces de comunicarse de manera inalámbrica, capacidad de procesamiento y autonomía propia.

Una Red Inalámbrica de Sensores o Wireless Sensor Network (WSN), es un conjunto de estos dispositivos que reciben el nombre de nodos-sensores de bajo costo y mínimo consumo y se comunican entre sí, formando una red inalámbrica. Esta tecnología inalámbrica tiene sus inicios en la década de 1970 a partir de proyectos surgidos y consolidados en terreno militar.

Entre los pioneros de estos sistemas destacan la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) que organizó el Taller de Redes de Sensores Distribuidos (Distributed Sensor Nets Workshop, DAR 1978), centrado en los desafíos de investigación de redes de sensores, tales como las tecnologías de redes, técnicas de procesamiento de señales y algoritmos distribuidos. Además, el Centro de Ciencias de Rockwell y la Universidad de Los Ángeles, ambas instituciones en los Estados Unidos no solo comenzaron el trabajo con los proyectos de redes, sino que también fueron los primeros centros de investigación en proponer un concepto oficial para la naciente tecnología (Dargie and Poellabauer, 2010).

El desarrollo además, por parte de un equipo científico de la Universidad de Carnegie Mellon de Pennsylvania, de un Sistema Operativo conocido como Accent, que permitía la comunicación y el acceso a los recursos necesarios para las WSN constituyó uno de los impulsos más significativos para la consolidación de las redes inalámbricas de transmisión (Wang and Balasingham, 2010).

Desde su surgimiento y hasta la fecha, las WSN han sido desarrolladas con el fin de aprovechar sus capacidades en diversas áreas de la ciencia y la vida cotidiana. Las aplicaciones de las redes sensoriales son tan numerosas, que engloban desde la monitorización de un campo de cultivo, el control de presión de los neumáticos de un automóvil, el seguimiento de animales en su hábitat natural para estudios genéticos, verificar las propiedades físicas de piezas críticas y equipos de industrialización, hasta el seguimiento médico de un paciente.

Si bien las redes de sensores poseen un amplio espectro de aplicaciones, aún constituyen una tecnología en plena evolución que requiere grandes investigaciones para su desarrollo y aplicación; pues este tipo de dispositivos nos abre un nuevo abanico de oportunidades para diseñar y crear todo tipo de aplicaciones, protocolos y sistemas capaces de facilitar el trabajo a los seres humanos a la vez que reducen sus costes.

Por ello, la presente investigación se centrará en las Redes Inalámbricas de Sensores, a partir de su utilización como mecanismo de seguridad en edificios de interés económico, político o social, en este caso la Universidad Central Marta Abreu de Las Villas y específicamente su Facultad de Ingeniería Eléctrica.

El presente estudio surge entonces desde la primicia de la inexistencia de un sistema capaz de monitorear problemas tales como la prevención o detección de incendios y la protección de los recursos materiales en la Facultad de Ingeniería Eléctrica.

La investigación plantea como objetivo general:

- Proponer una Red Inalámbrica de Sensores para edificios docentes.

Este objetivo general será desarrollado a partir de los siguientes objetivos específicos:

- Determinar los estándares más utilizados para Redes Inalámbricas de Sensores.
- Analizar diferentes redes WSN en edificios tanto comerciales como académicos.
- Diseñar una red WSN para un edificio docente.
- Evaluar el comportamiento de la red diseñada mediante técnicas de modelación y simulación.

Los objetivos trazados en este estudio responderán tres interrogantes científicas:

- ¿Qué características presentan las Redes Inalámbricas de Sensores?

- ¿Qué aplicaciones ofrecen estas redes?
- ¿Cuáles son las topologías más adecuadas para edificios docentes?

Además, dará cumplimiento a las tareas de investigación expuestas a continuación:

- Evaluación de las arquitecturas (componentes de software y hardware) que presentan las Redes Inalámbricas de Sensores.
- Selección del estándar de WSN a utilizar.
- Analizar las aplicaciones de las redes WSN para edificios docentes.
- Determinación de los sensores a utilizar en la aplicación tomando en cuenta el costo-beneficio.
- Análisis de diferentes variantes de redes en cuanto a topologías, sensores, equipos, etc.
- Evaluación del comportamiento o desempeño de la red para cada escenario.
- Analizar los resultados.

Esta investigación estará estructurada en tres capítulos:

- Capítulo I “Evaluación de las Redes Inalámbricas de Sensores”: incluye el resumen teórico sobre el tema y los conceptos principales a utilizar.
- Capítulo II “Procedimiento de Diseño de una WSN en un edificio docente”: expone la estrategia de instalación de cada uno de los dispositivos que forman la red en el edificio seleccionado, se analizan los problemas existentes entre las tecnologías Wi-Fi y ZigBee en la banda de 2.4Ghz y la solución dada a este problema.
- Capítulo III “Análisis del Desempeño de la Red WSN”: en el cual se presentará una simulación de la red propuesta en la herramienta OPNET Modeler 14.5, con el objetivo de analizar el desempeño de esta.

Capítulo I: Evaluación de las Redes Inalámbricas de Sensores

En este capítulo se tratan varios aspectos teóricos sobre las Redes Inalámbricas de Sensores (WSN) como son: los elementos componentes de una red de sensores, sus características, las estructuras de hardware y software de los nodos sensores, los estándares y protocolos de comunicaciones, las topologías, etc.

Además se analizan las aplicaciones que ofrecen las redes de sensores, particularizando en dos ejemplos.

1. 1. Generalidades sobre las Redes Inalámbricas de Sensores

Una red de sensores está formada por un número determinado de sensores. Estos pequeños nodos sensores son elementos de bajo coste y consumo, con unas capacidades muy específicas y limitadas de monitorización, procesamiento de datos y comunicación. Poseen la capacidad de auto-organizarse y comunicarse con otros nodos cercanos, de esta forma cualquier nodo de la red delega en otros la responsabilidad de reenviar la información, de forma que esta sea capaz de alcanzar su objetivo. En general, aunque no siempre es así, cada uno de los nodos juega dos papeles fundamentales en la red: Por una parte debe ocuparse de retransmitir datos recibidos de otros vecinos y, además, utilizar su limitada capacidad de proceso para tratar sus propios datos y determinar los datos que debe transmitir. (Navarro, 2010).

Una red de sensores se basa en la idea de construir un entorno donde un gran número de pequeños elementos (sensores) colaboren para llevar a cabo una tarea, que generalmente consiste en tareas de monitorización de uno u otro tipo, y suelen están formadas por un gran número de sensores desplegados en el fenómeno o cerca de fenómeno que desea observarse.

En la arquitectura básica de una red de sensores (Figura 1.1) se pueden distinguir tres elementos principales:

- **Campo de sensores:** formado por la zona cubierta por el conjunto de sensores de la red.
- **Administrador de Tareas:** donde pueden llevarse a cabo tareas de análisis, procesamiento y almacenamiento de datos o gestión activa de la red.
- **Nodo Sumidero (Sink) o Estación Base:** intermediario que se encarga de enlazar la red de sensores con el resto de las redes.

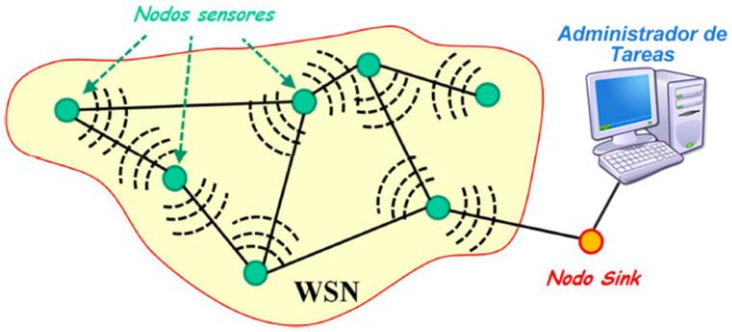
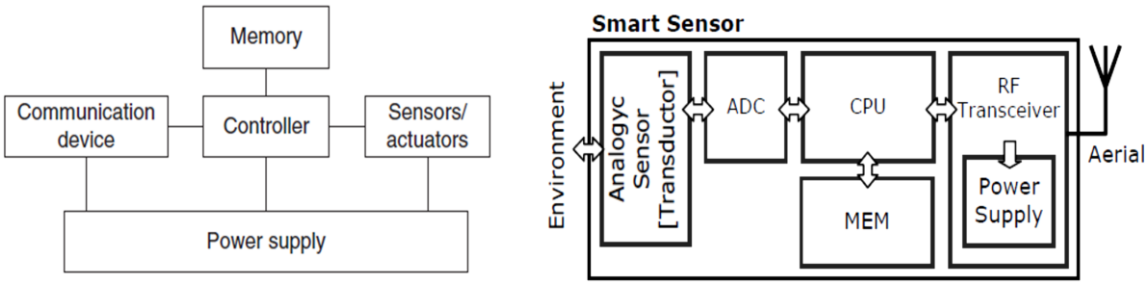


Figura 1.1: Arquitectura básica de una Red de Sensores. (Linares, 2014).

1. 2. Componentes de Hardware

Al elegir los componentes de hardware de un nodo sensor inalámbrico, evidentemente los requisitos de la aplicación juegan un factor decisivo en lo que respecta principalmente al tamaño, los costos y el consumo de energía de los nodos; facilidades de comunicación y cómputo, como tal, a menudo son considerados como de calidad aceptable, pero las compensaciones entre características y costos es crucial. (Karl and Willig, 2005).

Un nodo básico sensor consta de cinco componentes principales como bien se observa en la Figura 1.2:



a) Componentes fundamentales b) Estructura interna

Figura 1.2: Componentes fundamentales y estructura del hardware de un nodo sensor (Karl and Willig, 2005).

- **Controlador:** Es el núcleo de un nodo sensor inalámbrico. Recoge datos de los sensores, procesa estos datos, decide cuándo y dónde enviarlo, recibe datos de otros nodos de sensores, y decide sobre el comportamiento del actuador; es la unidad central de procesamiento (CPU) del nodo.
- **Memoria:** Es utilizada para almacenar programas y datos intermedios. Desde un punto de gasto de energía, las clases más relevantes de memoria son la memoria integrada en el chip de un microcontrolador y la memoria flash, la memoria RAM fuera del chip es raramente usada. Las memorias flash son usadas gracias a su bajo coste y su gran capacidad de almacenamiento.
- **Sensores y actuadores:** Son la interfaz real con el mundo físico: dispositivos que pueden observar o controlar los parámetros físicos del medio ambiente. Los sensores son dispositivos hardware que producen una respuesta medible ante un cambio en un estado físico, como puede ser temperatura o presión. Los sensores detectan o miden cambios físicos en el área que están monitorizando. En el Anexo I se presentan los diferentes tipos de sensores utilizados en redes de sensores inalámbricos así como sus principales características. (Linares, 2014).
- **Comunicación:** Los nodos en una red requieren un dispositivo para enviar y recibir información sobre un canal inalámbrico. Para el caso de la comunicación inalámbrica, la primera decisión que tomar es la del medio de transmisión, las opciones habituales incluyen frecuencias de radio, la comunicación óptica y ultrasonido; otros medios como la inductancia magnética sólo se utilizan en casos muy concretos. De estas opciones, Radio Frecuencia (RF) es, por mucho, la más

relevante, ya que es la que mejor se ajusta a los requisitos de la mayoría de las aplicaciones WSN, proporciona un alcance relativamente largo y altas velocidades de datos, una tasa de error aceptable, un gasto de energía razonable, y no requiere línea de vista entre el emisor y el receptor.

- **Fuente de alimentación:** Para los nodos sensores inalámbricos, la alimentación constituye un componente crucial. Hay dos aspectos esenciales: primero, el almacenamiento y suministro de energía en la forma requerida; segundo, intentar recargar esa energía consumida mediante alguna fuente externa de energía. Una forma convencional de energía es mediante baterías, como las clásicas AA, que almacena entre 2.2-2.5 Ah a 1.5 V.

1. 2. 1. Eficiencia energética

El objetivo de la eficiencia energética es maximizar el tiempo de vida de la red al mismo tiempo que la aplicación cumple con sus requisitos de QoS. Las mejoras tecnológicas que permiten aumentar la capacidad de las baterías progresan despacio. Esto quiere decir que la eficiencia energética seguirá siendo un reto para este tipo de redes en el futuro próximo.

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

La comunicación es el primer consumidor de energía. Un sistema distribuido significará que algunos sensores necesitarán comunicarse a través de largas distancias, lo que se traducirá en mayor consumo. Por ello, es una buena idea el procesar localmente la mayor cantidad de energía, para minimizar el número de bits transmitidos.

El CPU es capaz de quedar en estado “inactivo” (sleep) mientras “no tenga nada que hacer”. El envío de datos desde los nodos puede ser de tres formas: de modo continuo en los intervalos establecidos, dirigido por eventos (envía cuando se cumple cierta condición) o dirigido por consulta (solo cuando se le solicita). También hay sistemas híbridos que utilizan una combinación de los antes mencionados.

Para el ahorro de energía los nodos pasan por estos estados:

- **Inactivo (Sleep):** El nodo pasa la mayor parte del tiempo en este estado sin actividad.
- **Levantarse (Wakeup):** Es el tiempo de transición del estado de inactividad al estado activo y el mismo debe ser minimizado.
- **Activo (Active):** Debe estar el mínimo período de tiempo de trabajo y retornar de inmediato al estado inactivo.

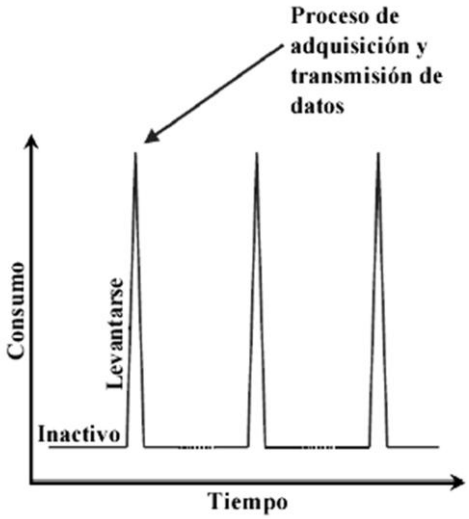


Figura 1.3: Estados de un nodo sensor

1. 3. Componentes de Software

El software que compone un nodo sensor debe garantizar que el objetivo de la aplicación se alcance. Los componentes de software deben superar las desventajas de recursos limitados del hardware en los nodos sensores.

La figura 1.4 muestra los componentes de software que caracterizan a un nodo sensor, partiendo desde el sistema operativo que se encuentra a nivel de nodo, al middleware y la aplicación que se distribuyen a lo largo de la red.

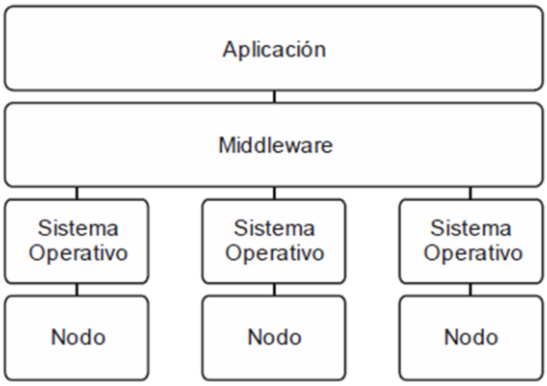


Figura 1.4: Capas de Software. (Reddy, 2009).

El sistema operativo en un nodo sensor es el medio por el que se accederá al hardware, gestionará el uso de memoria y de energía a través de comandos, y controlará los procesamientos que la aplicación requiere (Dong, 2010).

El middleware, es el intermediario entre los sistemas operativos y las aplicaciones. En redes de sensores inalámbricos, el middleware debe hacer frente a la restricción de recursos de los nodos, posibles ambientes hostiles, escalabilidad, etc (García-Hernando and Martínez-Ortega, 2008).

1. 3. 1. Sistemas Operativos

A continuación se enlistan los sistemas operativos para redes de sensores inalámbricos más utilizados:

- **TinyOS:** es un sistema operativo monolítico que utiliza el modelo de componente, esto significa, que de acuerdo a las necesidades de la aplicación, diferentes componentes pueden integrarse en una sola imagen. Cada componente incluye comandos, eventos y tareas (Farooq M, 2011). El ser de código abierto y operable en redes con marcadas limitaciones de memoria, ha provocado que sea uno de los sistemas operativos más populares. Actualmente cuenta con una gran comunidad de desarrollo. TinyOS es impulsado por eventos, ofrece servicios de distribución y herramientas de adquisición de datos (García-Hernando and Martínez-Ortega, 2008). Este sistema operativo debe su popularidad a su capacidad de adaptación a las marcadas limitantes de los nodos, como la memoria y la energía.

- **SOS:** se trata de un sistema operativo modular, en el que cada módulo representa una función específica, se diferencia de TinyOS en el alojamiento de memoria, mientras en TinyOS el alojamiento es estático, SOS permite una asociación de memoria dinámica (Dargie and Poellabauer, 2010).
- **Contiki:** es un sistema operativo modular de código abierto. Caracterizado por ser ligero y portátil, orientado a eventos y multitarea. Destaca una interfaz gráfica de usuario, un navegador y servidor web personal (Farooq M, 2011).
- **MagnetOS:** este sistema operativo permite reducir el gasto energético al realizar partición de código y colocar el código objeto a través de la red. Sin embargo, la característica que lo distingue, es el hecho de poseer un sistema único que simula la máquina virtual de Java, mismo que permite utilizar el lenguaje Java (García-Hernando and Martínez-Ortega, 2008).
- **LiteOS:** sistema operativo basado en hilos, a diferencia de otros sistemas operativos no brinda componentes o módulos, es decir, el sistema es una sola aplicación. Utiliza alojamiento de memoria dinámico y soporta múltiples aplicaciones (Dargie and Poellabauer, 2010).
- **NanoRK:** sistema operativo monolítico multitarea, brinda soporte para redes con múltiples saltos, utiliza muy pocos recursos de aplicación y acepta aplicaciones y programación en tiempo real (Farooq M, 2011).

1. 4. Estándares Inalámbricos

Debido al rápido desarrollo en el campo de las comunicaciones, cada vez más se están desarrollando y adoptando nuevas tecnologías, sobre todo, la tecnología inalámbrica que proporciona una manera más conveniente de transmisión de información que la cableada. En los últimos años, hubo un fuerte desarrollo en la comunicación inalámbrica. Tales como Wi-Fi para redes de área local, Bluetooth y ZigBee para redes de área personal y WiMAX para redes de área metropolitana (Yang and Yu, 2008). En este capítulo se hará un mayor énfasis en las tecnologías Wi-Fi y ZigBee, ya que serán los dos estándares a utilizar en la red propuesta.

1. 4. 1. Estándar IEEE 802.11

Las redes Inalámbricas de Área Local (Wireless LAN) se basan en el estándar IEEE 802.11 (IEEE, 2012), donde en el mismo se establecen las especificaciones para el nivel físico y para el control de acceso al medio.

Las Redes WLAN se han difundido ampliamente para dar cobertura a hogares, edificios de oficinas, campus docentes, instalaciones hospitalarias, aeropuertos, ferrocarriles, parques, etc. Posibilitando hoy en día una forma fácil de acceso a Internet.

El primer estándar que apareció para estas redes fue el estándar IEEE 802.11, posteriormente se desarrolló IEEE 802.11b. Tiempo después se empezó a desarrollar IEEE 802.11a pero se estaba buscando un estándar que fuera compatible con IEEE 802.11b, por lo que finalmente se desarrolló IEEE 802.11g. Los estándares IEEE 802.11g e IEEE 802.11a ofrecen las mismas tasas de transmisión, pero IEEE 802.11g tiene un mayor alcance debido a la frecuencia de operación. Debido a esto y su compatibilidad con IEEE 802.11b, el estándar IEEE 802.11g es el más utilizado. Recientemente se liberó el estándar IEEE 802.11n que opera a la misma frecuencia que IEEE 802.11a e IEEE 802.11b/g; antes de liberarlo se comercializaba bajo el nombre de “draft IEEE 802.11n” (Salvetti, 2012).

A continuación se mencionan las características más importantes de los estándares IEEE 802.11.

IEEE 802.11 (1997)

El estándar IEEE 802.11 inicialmente estableció dos técnicas de transmisión para radiofrecuencia: FHSS y DSSS, y una especificación de transmisión infrarroja que no ha sido desarrollada. FHSS es una tecnología de transmisión inalámbrica, que tiene como característica el salto o cambio de la frecuencia que utiliza para transmisión; el uso de frecuencias para su salto están determinadas por patrones y los saltos se realizan en toda la banda disponible. DSSS es una tecnología que siempre opera sobre el canal de frecuencia, de tal forma que no ocupa toda la banda disponible (Salvetti, 2012).

IEEE 802.11 puede utilizar tasas de transmisión de 1Mbps y 2Mbps. FHSS y DSSS son dos mecanismos que no son compatibles entre sí.

Al hablar de esta familia de estándares, si nos ubicamos dentro del modelo de interconexión de sistemas abiertos (OSI), decimos que las funciones que realizan se encuentran en las dos primeras capas (capa física y capa de enlace).

IEEE 802.11b (1999)

Este estándar es conocido como HR-DSSS. Es una mejora del primer estándar IEEE 802.11 publicado por la IEEE. La contribución de IEEE 802.11b fue el incremento de las tasas de transmisión de 5.5Mbps y 11Mbps. Para llevar a cabo esto, DSSS fue la técnica elegida para la capa física debido a que FHSS no puede soportar tasas de transmisión mayores a 2Mbps. IEEE 802.11b puede interoperar con sistemas IEEE 802.11 DSSS, pero no puede hacerlo con sistemas IEEE 802.11 FHSS. La diferencia principal entre DSSS y HR-DSSS radica en que utilizan diferentes métodos de modulación (IEEE, 1999b).

IEEE 802.11a (1999)

El estándar IEEE 802.11a, conocido como OFDM, utiliza frecuencias de transmisión cercanas a 5GHz; fue introducido al mismo tiempo que IEEE 802.11b. Es una tecnología que hace un multiplexado en el dominio de la frecuencia para transmitir datos, de tal forma que divide el canal de operación en varios canales y realiza transmisiones en paralelo. El sistema OFDM provee tasas de transmisión de hasta 54Mbps, pero tiene características de propagación diferentes a 802.11b debido a la frecuencia de uso (IEEE, 1999a).

IEEE 802.11g (2003)

El estándar IEEE 802.11g, conocido como ERP-OFDM, soporta tasas de transmisión de hasta 54Mbps, utilizando técnicas de modulación provenientes de IEEE 802.11a. Adicionalmente al uso ERP-OFDM, el estándar IEEE 802.11g puede utilizar un modo de operación llamado ERP-DSSS, que básicamente establece compatibilidad con IEEE 802.11b (HR-DSSS) (IEEE, 2003).

IEEE 802.11n (2009)

Este estándar se basa en la utilización de varias antenas de forma simultánea, teniendo hasta un máximo de cuatro para recepción y cuatro para transmisión, esta característica se le conoce como MIMO (Multiple Input Multiple Output).

El estándar, conocido como HT-OFDM, realiza transmisiones simultáneas en las que aplica un multiplexado en el dominio de la frecuencia (MIMO-OFDM), de tal forma que se pueden realizar varias transmisiones sobre la misma frecuencia al mismo tiempo con antenas diferentes. IEEE 802.11n tiene varios modos de operación, lo que da como resultado compatibilidad con IEEE 802.11a y IEEE 802.11g. En el primer modo opera de forma compatible con IEEE 802.11a ó IEEE 802.11g, dejando a un lado la operación IEEE 802.11n. En el segundo modo la forma de operación es mixta. IEEE 802.11n opera con los protocolos IEEE 802.11a e IEEE 802.11g de forma simultánea. En el último modo la operación es solamente como IEEE 802.11n. Teóricamente con la utilización de esta tecnología se pueden alcanzar tasas de transmisión cercanas a 600Mbps (IEEE, 2009).

IEEE 802.11ac (2013)

El IEEE 802.11ac adopta muchas propiedades del IEEE 802.11n, como por ejemplo la codificación de canal o los modos MIMO. A ello se añaden anchos de banda de 80 MHz y 160 MHz (en el IEEE 802.11n hasta ahora solo 40 MHz), 256QAM, hasta ocho antenas así como MIMO multiusuario. Con un ancho de banda de 80 MHz, una antena y 64QAM 5/6 se alcanza ya una velocidad de transmisión bruta de 293 Mbps; todos los equipos conformes al IEEE 802.11ac deben soportar este modo. En modos opcionales se pueden alcanzar bajo condiciones óptimas, con 256QAM y ocho antenas, velocidades brutas de 3,5 Gbps. El IEEE 802.11ac está previsto únicamente para las bandas de 5 GHz no sujetas a licencia, la banda ISM (Industrial Scientific Medical) de 2,4 GHz, utilizada hasta ahora casi siempre para WLAN, ya no está incluida. Permite velocidades de al menos 1.000 Mbps en la banda de los 5 gigahercios, esa banda al principio restringida a edificios oficiales, como embajadas (IEEE, 2013).

Radiofrecuencias disponibles

La Comisión Federal de Comunicaciones (FCC) ha creado dos bandas de uso libre, conocidas como: bandas Industrial, Científico y Médico (ISM) y las bandas de Infraestructura de Información Nacional sin Licencia (U-NII). Actualmente existen 12 bandas ISM, pero solo la que empieza en 2.4GHz es utilizada por los estándares IEEE 802.11, IEEE 802.11bg y IEEE 802.11n, mientras que las cuatro bandas U-NII son

utilizadas por IEEE 802.11a y IEEE 802.11n. En la Tabla 1.1 se muestra el desglose de estas bandas y como se relacionan con los estándares IEEE 802.11 (Salvetti, 2012).

Estándar	Frecuencia y Banda de Operación
IEEE 802.11	2.4GHz ISM
IEEE 802.11a	5GHz U-NII
IEEE 802.11b	2.4GHz ISM
IEEE 802.11g	2.4GHz ISM
IEEE 802.11n	2.4GHz ISM ó 5GHz U-NII

Tabla 1.1: Bandas y Frecuencias utilizadas por los estándares 802.11.

Canales de Operación

El rango de frecuencias 2.4GHz a 2.5GHz se encuentra dividido en canales de un ancho definido, los cuales fueron establecidos por los organismos reguladores de las telecomunicaciones de cada país (Figura 1.5).

La selección de los canales en el diseño de las redes IEEE 802.11 es indispensable. Para evitar interferencia creada por los mismos elementos de una red, es necesario seleccionar canales cuyas frecuencias no se traslapen. La separación que existe entre los canales 1 y 6, y los canales 6 y 11 es mayor a 22MHz, razón por la cual son los más utilizados.

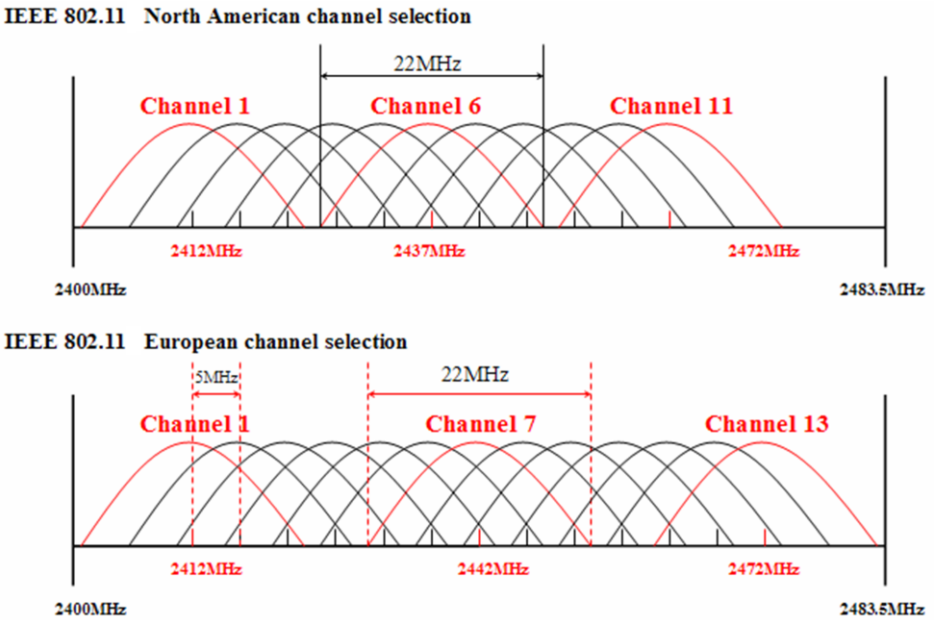


Figura 1.5: Selección de canales IEEE 802.11 para la banda de 2.4GHz (Yang and Yu, 2008).

1. 4. 2. Estándar IEEE 802.15.4

El estándar IEEE 802.15.4, cuya última revisión se aprobó en 2006, define una capa de comunicación que se encuentra en el nivel 2 (Enlace de datos) del modelo OSI (IEEE, 2011). Aquí las unidades de la información digital (bits) son gestionados y organizados para convertirse en impulsos electromagnéticos (ondas) en el nivel inferior, el físico. Su objetivo principal es permitir la comunicación entre dos dispositivos. La característica más importante de este estándar es su flexibilidad de red, bajo coste, bajo consumo de energía.

Este estándar fue creado para llenar el hueco existente en el campo de estándares inalámbricos de baja tasa para aplicaciones en redes de sensores. Los estándares existentes hasta el momento en el mercado estaban destinados a aplicaciones con mayores requisitos en cuanto a ancho de banda se refiere, como pueden ser videoconferencias o redes domésticas. (Carbajal, 2012).

El requisito fundamental del estándar IEEE 802.15.4 es un consumo de potencia extremadamente bajo. La eficiencia energética de este protocolo reside fundamentalmente en el uso de las tramas de Faro o Indicadoras (Beacon), que permiten sincronizar los dispositivos de la red para que puedan permanecer en modo ahorro de energía el mayor tiempo posible, esto supone una gran ventaja para el desarrollo WSN que realicen tanto tareas de monitorización como de control. El inconveniente es que, debido al bajo consumo de potencia, el radio de cobertura se ve reducido. (Carbajal, 2012).

Las frecuencias definidas por el estándar IEEE 802.15.4 se reparten entre los 27 canales disponibles y las bandas de frecuencias respectivas que se muestran en la Tabla 1.2.

Banda RF	Rango de frecuencias (MHz)	Tasa de datos		Número de canal	Área geográfica
		Kbps	Ksímbolos/s		
868 MHz	868,3	20	20	0(1 canal)	Europa
915 MHz	902-928	40	40	1-10 (10 canales)	América, Australia
2400 MHz	2405-2480	250	62,5	11-26 (16 canales)	Todo el mundo

Tabla 1.2: Bandas de frecuencia utilizadas por el estándar IEEE 802.15.4

La tecnología inalámbrica basada en IEEE 802.15.4 permite comunicaciones de corto alcance con distancias de hasta 75 m y bajo consumo; está diseñado para utilizar bandas de frecuencia sin licencia. Pueden funcionar en las bandas 868 MHz, 915 MHz y 2400 MHz, aunque la banda de 2400 MHz es la más utilizada por las siguientes razones:

- Uso sin licencia disponible en todo el mundo.
- Tasa de datos más alta y mayor número de canales.
- Menor consumo de potencia (debido a que se tarda menos tiempo en enviar y recibir porque la tasa de datos es más alta).
- Banda de frecuencias comúnmente empleada en el mercado (también utilizada por Bluetooth y el estándar IEEE 802.11).

Las técnicas que utiliza este estándar para evitar que todos los nodos emitan al mismo tiempo son:

- CSMA-CA: Cada nodo debe analizar la red antes de transmitir. Si la energía más alta se encuentra en un nivel específico, el nodo espera al transceptor durante un tiempo al azar e intenta de nuevo.
- GTS: La segunda es una garantía de tiempo. Este sistema utiliza un nodo central (PAN coordinador), que da las franjas horarias de tiempo para cada uno de los nodos de modo que cualquier nodo sabe cuándo tiene que transmitir.

El canal 0 se asigna a la banda de 868 Mhz con frecuencia central en 868.3 Mhz (Dignani, 2011). La frecuencia central en cada canal de la banda de 915Mhz se calcula:

FREC. central [Mhz]= 906 + 2 * (Nº canal -1)

Con $1 \leq$ Nº canal ≤ 10

Para la banda de 2.4 GHz la frecuencia central se calcula:

Frecuencia central [MHz]= 2405 + 5 * (Nº canal -1)

Con $11 \leq$ Nº canal ≤ 26

La banda de 2.4 GHz es la que dispone de más ancho de banda, está dividida en 16 canales de 2 MHz cada uno y una separación entre canales de 5 MHz, para evitar así la interferencia co-canal, como puede apreciarse en la figura 1.6.

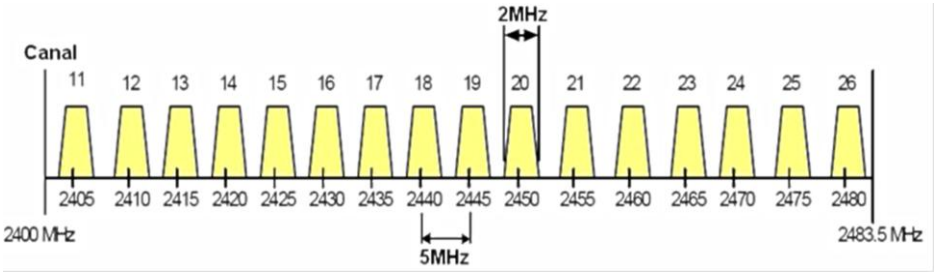


Figura 1.6: División espectral de canales en la banda de 2.4Ghz (Dignani, 2011).

Arquitectura del estándar IEEE 802.15.4

La arquitectura definida en el estándar IEEE 802.15.4 se divide en dos niveles: capa física y subcapa MAC (junto con la subcapa LLC). El conjunto de subcapa MAC y subcapa LLC se conoce como capa de enlace de datos.

La arquitectura descrita se muestra en la Figura 1.7:

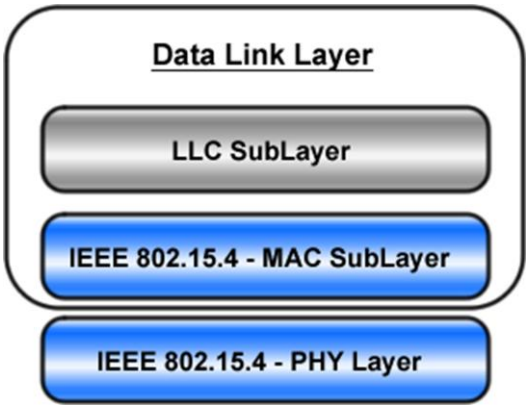


Figura 1.7: Arquitectura de IEEE 802.15.4 (IEEE, 2011).

A continuación se definen las funciones y servicios de ambas capas:

Capa física

La capa física actúa como interfaz con el medio físico de transmisión, radio en este caso, e intercambia bits de datos con el medio y con la capa superior, la subcapa MAC.

Las funciones de la capa física con el medio son las siguientes:

- Estimación del canal.
- Comunicaciones a nivel de bit (modulación y demodulación de bits y sincronización de paquetes).

La capa física ofrece a la subcapa MAC los siguientes servicios:

- PHY Data Service: proporciona un mecanismo de envío de datos a la subcapa MAC.
- PHY Management Services: proporciona mecanismos para controlar la configuración y la funcionalidad de las comunicaciones radio a la subcapa MAC.

La información necesaria para gestionar la capa física se almacena en una base de datos llamada PHY PIB.

Subcapa MAC

Las funciones principales de la subcapa de control de acceso al medio (MAC) son las siguientes:

- Proporcionar servicios para que los dispositivos puedan asociarse o desasociarse de la red.
- Proporcionar control de acceso a los canales compartidos.
- Generación de beacons, si procede.
- Gestión de Guaranteed Timeslot (GTS), si procede.

La subcapa MAC ofrece a la capa superior los siguientes servicios:

- MAC Data Service (MCPS): proporciona un mecanismo de envío de datos a la capa superior.
- MAC Management Services (MLME): proporciona mecanismos para controlar la configuración y la funcionalidad de las comunicaciones radio y de red de la capa superior.

La información necesaria para gestionar la subcapa MAC se almacena en una base de datos llamada MAC PIB.

1. 4. 3. Estándar ZigBee

ZigBee es un estándar que define un conjunto de protocolos para el armado de redes inalámbricas de corta distancia y baja velocidad de datos. Opera en las bandas de 868 MHz, 915 MHz y 2.4 GHz y puede transferir datos hasta 250Kbps. (Dignani, 2011)

Este estándar fue desarrollado por la Alianza ZigBee (ZigBee Alliance, 2011), que tiene a cientos de compañías desde fabricantes de semiconductores y desarrolladores de software a constructores de equipos OEMs e instaladores. Esta organización sin fines de lucro nace en el año 2002.

En la figura 1.8 se muestran las capas del protocolo ZigBee. Estas se basan en el modelo de referencia ISO para interconexión de sistemas abiertos OSI. Este modelo cuenta con 7 capas pero ZigBee usa solo 4 capas con el objetivo de simplificar la arquitectura para el armado de una red de baja tasa de transmisión, simple y de bajo consumo. Las 2 capas inferiores, o sea la capa física (PHY) y la capa de acceso al medio (MAC) son las definidas por el estándar IEEE 802.15.4. Las capas de red (NWK) y de aplicación (APL) se definen en ZigBee. Cada capa se conecta con las capas adyacentes por medio de un SAP (Service Access Point). Un SAP es un lugar por donde una capa superior requiere un servicio a una capa inferior.

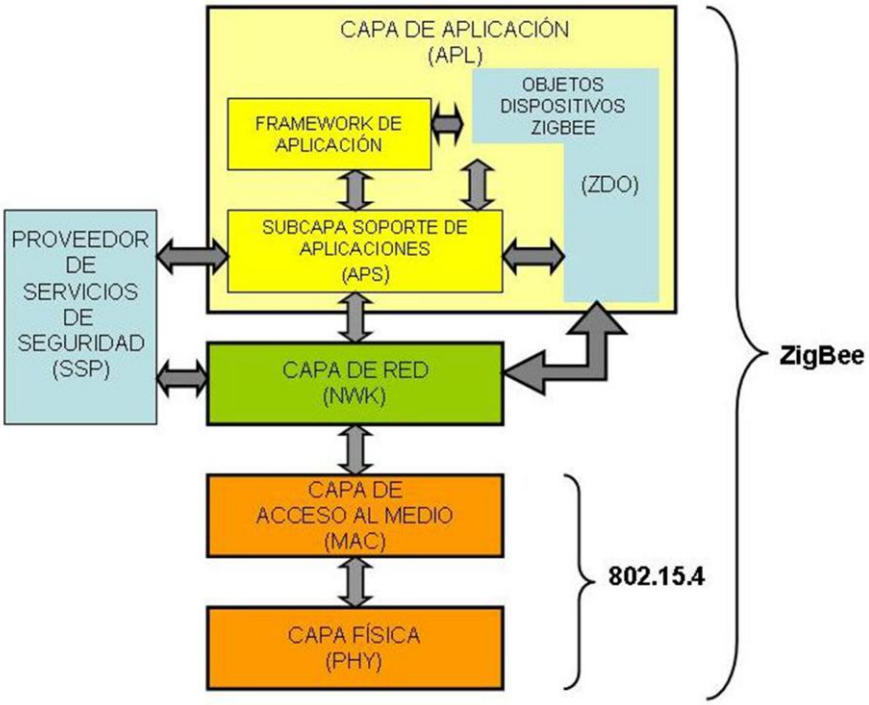


Figura 1.8: Arquitectura de ZigBee (ZigBee Alliance, 2011).

Capa de Red ZigBee

La capa de red provee a Zigbee funciones para el armado y manejo de redes y una interfaz simple para relacionarla con las aplicaciones de los usuarios. Las tareas más importantes de la capa de red son:

- Establecer una nueva red brindando topologías como árbol ó malla.
- Agregar o quitar a un dispositivo a/de la red.
- Garantizar la comunicación dentro de toda la red más allá del alcance de un único nodo.
- Configurar a un nuevo dispositivo para que pueda operar en la red.
- Asignar direcciones de red a los dispositivos brindando una interfase unificada para todos ellos.
- Sincronizar entre dispositivos usando balizas ó encuestas.
- Proveer seguridad.
- Encaminar (Rutear) tramas a sus destinos.

Capa de aplicación

Consiste en la subcapa APS (Application Support) y la ZDO (ZigBee Device Object). Responsabilidades: mantener las tablas para los enlaces (binding) que consiste en balancear o adaptar dos dispositivos entre ellos basados en los servicios y necesidades.

Cada subcapa se puede definir con:

- APS: trata de descubrir también a otros dispositivos que están operando en su mismo espacio operativo.
- ZDO: Define el rol de un dispositivo dentro de la red.

En la capa de aplicación se inician o responden pedidos de enlace y se establece una relación segura entre dispositivos seleccionando un método de seguridad como una clave.

1. 5. Topologías de red

Dos tipos de dispositivos diferentes pueden participar en una red IEEE 802.15.4: un Dispositivo de Función Completa (FFD) y un Dispositivo de Función Reducida (RFD). Un

dispositivo FFD es capaz de servir como un coordinador de red de área personal (PAN Coordinator) o coordinador. Un dispositivo RFD no es capaz de servir ya sea como un coordinador de PAN o un coordinador. Una red WPAN incluye al menos un dispositivo FFD, que funciona como el coordinador de la red PAN (IEEE, 2011).

En la topología en estrella, se establece la comunicación entre los dispositivos y un solo controlador central, llamado el coordinador de la red PAN. Las aplicaciones que se benefician de una topología en estrella incluyen domótica, periféricos de PC, juegos, y cuidado de la salud personal.

La topología de punto a punto también cuenta con un coordinador de red PAN; sin embargo, se diferencia de la topología en estrella en que cualquier dispositivo es capaz de comunicarse con cualquier otro dispositivo, siempre y cuando están en el rango de uno al otro.

1. 5. 1. Formación de una red en estrella

La estructura básica de una red en estrella se ilustra en la Figura 1.9. Después de activar un dispositivo FFD, se puede establecer su propia red y convertirse en el coordinador de la red PAN. Todas las redes en estrella operan independientemente de todas las otras redes en estrella actualmente en operación. Esto se logra mediante la elección de un identificador PAN que no se utiliza actualmente por cualquier otra red dentro del rango de radiocomunicaciones. Una vez elegido el identificador PAN, el coordinador de la red PAN permite que otros dispositivos, potencialmente ambos dispositivos FFDs y RFDs, se unan a su red. (IEEE, 2011).

1. 5. 2. Formación de una red punto a punto

En una topología de punto a punto, cada dispositivo es capaz de comunicarse con cualquier otro dispositivo dentro de su rango de radiocomunicaciones. Un dispositivo está nominado como el coordinador de red PAN, por ejemplo, en virtud de ser el primer dispositivo para comunicarse en el canal. Otras estructuras de red se construyen fuera de la topología de punto a punto, y es posible imponer restricciones topológicas en la formación de la red. La estructura de esta red se muestra también en la Figura 1.9.

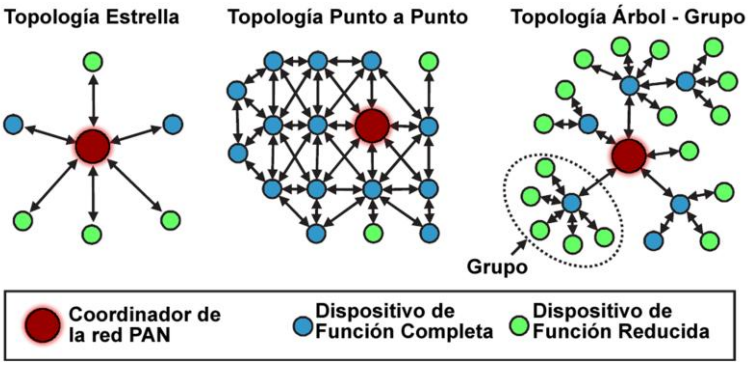


Figura 1.9. Topologías de red. (Kuorilehto et al., 2007).

Un ejemplo del uso de la topología de punto a punto es el árbol-clúster. La red de Árbol-Grupo es un caso especial de una red punto a punto en la que la mayoría de los dispositivos son FFDs. Un dispositivo RFD se conecta a una red árbol-clúster como un dispositivo hoja al final de una rama porque los RFDs no permiten que otros dispositivos se asocien. Cualquier dispositivo FFD es capaz de actuar como un coordinador y proporcionar servicios de sincronización a otros dispositivos u otros coordinadores. El coordinador de red PAN forma el primer clúster seleccionando un identificador PAN sin usar y transmitiendo tramas de señalización a los dispositivos vecinos. La ventaja de una topología árbol-clúster es que incrementa el área de cobertura, mientras que la desventaja es un aumento en la latencia del mensaje.

1. 6. Estudio comparativo de Zigbee con otras tecnologías

En secciones anteriores se realizó una generalización del estándar ZigBee y de cómo éste opera y funciona sobre las dos capas inferiores, o sea la capa física (PHY) y la capa de acceso al medio (MAC) definidas por el estándar IEEE 802.15.4. Pero ZigBee no es el único que rige a las redes inalámbricas de sensores, existen mundialmente varios estándares además de ZigBee que usan el IEEE802.15.4 como base de su protocolo, entre ellos los más conocidos son 6LoWPAN y WirelessHART. También existen otros protocolos que no usan IEEE802.15.4 donde se destacan entre éstos Z-wave, Bluetooth y ULP Bluetooth (Dignani, 2011).

1. 6. 1. Wi-Fi

Un aspecto importante a resaltar es que, ni ZigBee, ni ningún otro estándar mencionado anteriormente, resulta el más indicado en aspectos como video vigilancia (o alguna otra aplicación en la que se necesite transmitir video de buena definición), tema muy importante en el desarrollo de este trabajo. Investigaciones han demostrado que resulta muy poco factible utilizar ZigBee para transmitir video de alta resolución debido a las características físicas de este estándar: bajo ancho de banda, baja razón de transmisión, reducido consumo de energía, poca capacidad de cómputo y de memoria de almacenamiento, etc. (Gasparini, 2010). Un ejemplo típico que evidencia la anterior afirmación sería el de un nodo sensor de video operando bajo el estándar ZigBee, encargado de monitorear los autos por una autopista. Si un auto pasase a unos 130 km/h, debido a la baja razón de cuadros por segundo que presenta este nodo sensor, para hacer una grabación de calidad se necesitaría ubicar este nodo más lejos de la carretera para poder grabar correctamente unos cuantos cuadros de la imagen, sin embargo a mayor distancia, menor calidad de imagen, debido a que ZigBee posee poca capacidad de cómputo y le sería inútil procesar imágenes de alta resolución captadas por cualquier lente.

Hoy en día, lo que resulta más factible para aplicaciones de video vigilancia de manera inalámbrica, es utilizar Wi-Fi para la captación de video bajos los estándares IEEE 802.11b/g/n y el utilizar ZigBee para captar magnitudes escalares como velocidad, temperatura y presión. Muestra de esto son los ejemplos a analizar en la sección 1.7. La red propuesta en el presente estudio está basada en la utilización de esta estrategia de diseño.

1. 6. 2. Bluetooth

Es inevitable la comparación entre dos estándares de redes WPAN. Bluetooth es un protocolo que se ha popularizado en los últimos años (Bluetooth, 2011). Su objetivo de diseño fue la eliminación de cables de interconexión de datos entre equipos de consumo masivo.

En primer lugar, Zigbee fue diseñado pensando en paquetes pequeños, por ejemplo, para paquetes de menos de 75 bytes, Zigbee tiene, a pesar de su baja velocidad física de transmisión de datos, una velocidad efectiva mayor que Bluetooth. Por lo tanto, para

pequeños paquetes Bluetooth va a gastar mayor energía debido a que necesita mayor tiempo de transmisión/recepción.

Además, el protocolo Bluetooth se basa en encuestar a cada dispositivo esclavo y en cambio Zigbee se basa en CSMA-CA, que debe esperar a tener el canal libre. Esto no representa un problema porque en redes de muy bajo tráfico como redes de sensores, no hay competencia por el canal.

En conclusión ZigBee y Bluetooth son dos soluciones pensadas para aplicaciones diferentes. Bluetooth es apto para aplicaciones de baja latencia como audio y video, es un protocolo maestro-esclavo para unos pocos dispositivos. Zigbee, por el contrario, está diseñado para uso de sensores que usan mensajes cortos y preparado para redes tipo estrella, malla o árbol entre cientos de dispositivos (Dignani, 2011).

1. 6. 3. 6LoWPAN

La filosofía de este protocolo es poder transmitir paquetes de tipo Ipv6 para simplificar la interfase entre redes de sensores e Internet (6LoWPAN, 2012). La ventaja natural es la facilidad de conexión de la red WPAN a Internet. La desventaja es que los nodos de sensores tienen limitaciones en capacidad de procesamiento. IPV6 requiere soporte de paquetes más grande que lo que brinda IEEE 802.15.4. El payload máximo de IEEE 802.15.4 es de 128 bytes contra 1280 bytes requeridos por IPV6 por lo que requiere una fragmentación. Para eso se agrega una capa en 6LoWPAN llamada capa de adaptación que fragmenta y rearma los paquetes.

La comparación con ZigBee indica que para aplicaciones de paquetes pequeños con baja interacción con dispositivos IP es más eficiente ZigBee. La interacción con Internet la puede hacer un dispositivo puente.

1. 6. 4. WirelessHart

HART es un protocolo usado en la industria para control de procesos, diagnóstico y control (WirelessHART, 2009). Es un protocolo para usar en redes cableadas. WirelessHart es la extensión a redes inalámbricas que usa la banda de 2.4 GHz y para seguridad aplica AES-128 tal como ZigBee. Si bien usa la misma base de IEEE 802.15.4 que ZigBee, utiliza

potencias más elevadas, y programa la capa física para poder hacer saltos de canal paquete a paquete. Tanto ZigBee como WirelessHart se usan en ambientes industriales. La ventaja de este último protocolo es la compatibilidad hacia atrás con las redes HART.

1. 6. 5. Z-wave

Fue desarrollado por la Alianza Z-wave (Z-wave Alliance, 2008). No adopta IEEE 802.15.4. Usa la banda de 900MHz en un sistema de banda angosta. Usa FSK con velocidad de datos de 40kbps. Z-Wave soporta direccionamiento de 8 bits contra los 16 bits de direccionamiento de ZigBee. Usa una variante de DES (Data Encryption Standard) como método de seguridad. Para algunas aplicaciones esta seguridad puede ser insuficiente ya que usa una clave de solo 56 bits. ZigBee ofrece más velocidad, seguridad y mayor cantidad de nodos en una red. Z-wave es más simple y consecuentemente tiene más bajo costo por nodo.

1. 6. 6. ULP Bluetooth

Ya se comparó ZigBee con Bluetooth y se remarcó el gran gasto energético de este último. ULP Bluetooth es un estándar desarrollado para comunicaciones con bajo ciclo efectivo con el objeto de reducir el consumo energético. ULP no soporta redes tipo malla. ULP compite con ZigBee en aplicaciones punto a punto. Hay algunos dispositivos Bluetooth llamados de modo dual que pueden hacer de interfase entre los dispositivos ULP y los Bluetooth clásicos ya que trabajan en los dos modos.

1. 7. Ejemplos de redes híbridas ZigBee/Wi-Fi

En esta sección se analizarán algunos ejemplos de redes híbridas ya existentes en el mundo que emplean ambas tecnologías, tanto Wi-Fi como ZigBee y la aplicación que se le puede dar a cada una, para sacar de ellas el mejor beneficio posible.

1. 7. 1. Monitoreo de Turbinas de viento generadoras de electricidad

Hoy en día, existe un auge en el desarrollo de tecnologías de energía renovable y prioritariamente la energía eólica. Los avances tecnológicos han facilitado la construcción de nuevas turbinas de viento de mayor tamaño y eficiencia. Debido a estos avances y al incremento cada día mayor de la cantidad de turbinas en funcionamiento, es necesario además un desarrollo en las tecnologías de monitoreo y control de estas estaciones mediante el uso de varias tecnologías como Ethernet, Wi-Fi y ZigBee. (Ahmed and Kim, 2013).

Para el monitoreo exitoso de cada estación generadora de electricidad, se ha hecho un despliegue estratégico de dispositivos dentro de la estación. En la Figura 1.10 se puede apreciar con mayor detalle la ubicación de cada dispositivo en cada una de las turbinas de viento.

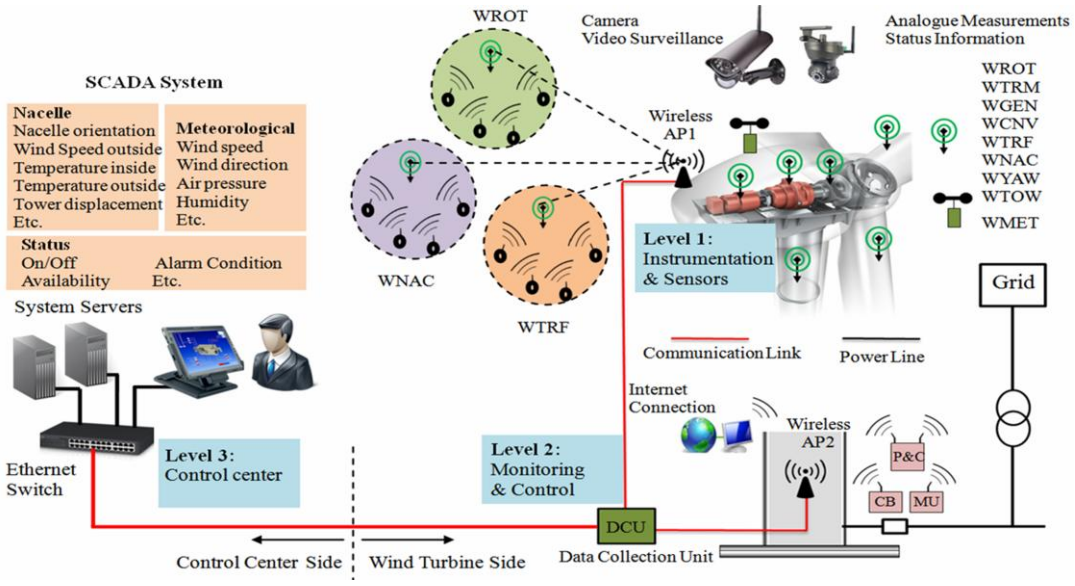


Figura 1.10: Vista esquemática del modelo de red híbrido (Ahmed and Kim, 2013).

En el caso de los dispositivos ZigBee, estos han sido colocados en lugares como el rotor de la turbina, el transformador y el generador, con el objetivo ad adquirir, procesar y transmitir datos hacia la estación central de monitoreo. Se utiliza para ello una topología en estrella entre un coordinador ZigBee y varios dispositivos sensores encargados de medir factores

físicos como velocidad del rotor, niveles de grasa, torque, vibración, temperatura, humedad, presión, dirección y velocidad del viento, voltaje y frecuencia.

Por otro lado se hace uso de la tecnología Wi-Fi mediante cámaras de video vigilancia, encargadas de realizar un escaneo constante de la zona, utilizando video de alta resolución e incluso visión térmica, (Figura 1.11) enviando los datos hacia un Access Point colocado dentro de la propia turbina.

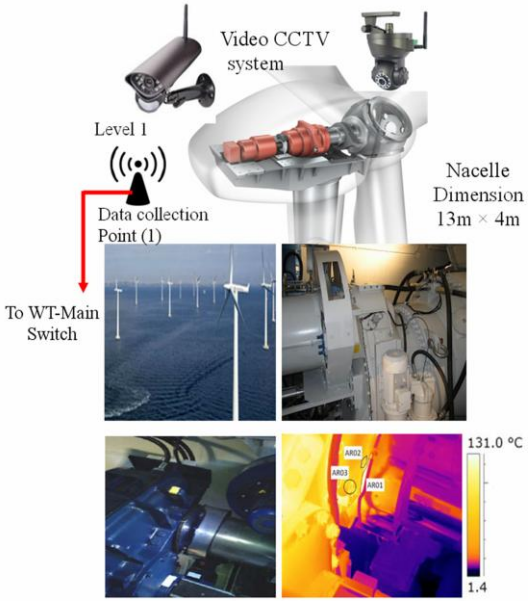


Figura 1.11: Subred de Video vigilancia (Ahmed and Kim, 2013).

Ambas tecnologías ofrecen conexión a Internet, permitiéndoles a los ingenieros una mayor facilidad de control y monitoreo de forma remota.

1. 7. 2. Automatización del hogar

Es una de las aplicaciones más usadas de este tipo de redes Wi-Fi - ZigBee ya que es muy fácil la instalación de dispositivos y la modificación de posición de los mismos (Dignani, 2011). Los usos típicos son:

- **Seguridad:** Sensores de movimiento, de rotura de cristales, apertura de puertas y ventanas. Además se incorporan cámaras IP capaces de filmar sucesos a una relativamente alta resolución.
- **Lectura de instrumentos de servicios:** Los medidores de consumo de agua, gas y energía eléctrica deben leerse en forma regular a efecto de facturar los servicios. Es

posible crear una red tipo malla para que la información de los medidores llegue directamente a la empresa de servicio. También los medidores ZigBee podrían comunicarse con los artefactos dentro de la casa. Por ejemplo ante un pico de consumo eléctrico se podría desconectar algún equipo de alto consumo.

- **Sistema de riego automático:** El uso de un medidor de humedad de suelo permite mejorar la eficiencia del consumo de agua. Se puede distribuir una red de sensores de humedad en un parque de modo que solo se riegue las zonas secas y controlar el tiempo de regado. Una red inalámbrica de sensores facilita enormemente la instalación y el mantenimiento.
- **Control de iluminación:** Para poder controlar el encendido de una lámpara se necesita un cableado a una llave interruptora en una caja de una pared. ZigBee simplifica la instalación de nuevas lámparas ó controles en lugares donde no está la cañería para pasar un cable. Si bien el costo de la conexión inalámbrica es más elevado que el convencional cableado, brinda otras ventajas además de la facilidad de instalación. Es posible conectar un controlador inteligente que encienda/apague luces de acuerdo a una programación, la detección de presencia de personas ó algún otro criterio.

Hoy en día, gracias a los avances de la tecnología, es más sencillo controlar y monitorear esta red mediante un solo dispositivo, el cual puede funcionar simultáneamente como Coordinador de la red ZigBee y como Access Point para la conexión inalámbrica con las cámaras instaladas en el hogar. El propietario del hogar puede monitorear incluso desde su Smartphone el buen funcionamiento de la seguridad de su hogar. Este ejemplo puede ser apreciado en la Figura 1.12:

Figura 1.12: Configuración típica de un sistema de automatización de un hogar. (Alibaba Group, 2014).

1. 8. Conclusiones del capítulo

Tras haber estudiado a fondo las redes de sensores inalámbricos, se observa que:

- Mundialmente los estándares más empleados en aplicaciones de video vigilancia de manera inalámbrica son el IEEE 802.11b/g/n para la captación de video de alta resolución y ZigBee para captar magnitudes escalares.
- Debido a las excelentes características de este tipo de redes, en la actualidad se están utilizando las redes de sensores en infinidad de proyectos relacionados con distintos campos como pueden ser: medio ambiente, salud, el ámbito militar, construcción y estructuras, automoción, domótica, agricultura, etc.
- Gracias a la utilización de esta tecnología en los diversos campos se está alcanzando un mayor nivel de control y monitorización lo cual lleva a una mejora del manejo del medio en que se están utilizando y dé respuesta frente a inconvenientes o simplemente para el perfeccionamiento del mismo.

Capítulo II: Procedimiento de Diseño de una WSN en un edificio docente

En este capítulo se aborda un análisis de las Redes WSN en edificios comerciales y académicos. En especial se describen los pasos a seguir en el diseño de una Red WSN para un edificio docente considerando la coexistencia entre la tecnología WiFi y ZigBee, dado que ambas comparten la banda de 2.4 GHz.

2. 1. Selección de la banda de frecuencia

En lo referente a los nodos sensores bajo el estándar ZigBee, casi todos los productos usan la banda de 900 – 928 Mhz y la de 2.4 – 2.483 Ghz sin embargo se presentan complicaciones en ese sentido incluso debido a que por ejemplo en Europa la banda de 900 – 928 Mhz es parte de la banda para comunicaciones móviles celulares GSM, por lo cual ellos utilizan la banda de 868 – 870 Mhz.

Luego de un análisis realizado a estas bandas de frecuencia (Tabla 1.2) se ha decidido el no utilizar la banda de 868 Mhz ya que esta banda solo permite una tasa de transmisión de 20 kbps, cosa que no es factible en la red que se propone implementar en este capítulo debido a la gran cantidad de nodos sensores que esta posee. Por otro lado también se puede desechar la banda de 915 Mhz ya que además de Europa, también en Cuba es parte de la banda de comunicaciones móviles celulares.

Por las razones antes mencionadas se ha decidido utilizar la banda de 2.4 Ghz, además la tendencia del mercado es por el uso de ésta banda que está libre en casi todo el mundo y que permite comunicarse con otros elementos inalámbricos de diferentes estándares que se pudieran acoplar a la red.

2. 2. Coexistencia entre Wi-Fi y ZigBee

Wi-Fi y ZigBee impactarán entre sí porque ambos utilizan la banda ISM de 2.4GHz. Al igual que en el capítulo anterior se mencionó, el estándar IEEE 802.15.4 define 16 canales que son separados 5MHz unos de otros, con un ancho de banda de cada canal de 2 MHz;

mientras que la norma IEEE 802.11b define 14 canales dentro de la banda de 2,4 GHz, con una distancia de 5MHz entre dos canales adyacentes. Dado que la señal de radio WLAN tiene un ancho de banda de 22MHz, no todos los canales se pueden utilizar al mismo tiempo. De hecho, sólo tres canales WLAN que no se solapan se pueden utilizar simultáneamente. Para América del Norte se utilizan los canales 1, 6 y 11 y para Europa 1, 7 y 13. La Figura 2.1 ilustra la selección de canales para IEEE 802.11 e IEEE 802.15.4, así como el solapamiento entre ellos.

Muchas han sido las investigaciones realizadas con el objetivo de analizar la coexistencia entre ambas normas, basándose en aspectos como la probabilidad de error de bit (BER) y de paquete (PER), la distancia óptima que debe existir entre los dispositivos que usen estándares contrarios, así como el tamaño máximo de cada paquete a enviar.

Resultados de estas investigaciones han demostrado que cada canal de Wi-Fi solapa hasta 4 canales de ZigBee, si este último transmite dentro de cualquiera de estos canales solapados, estaría expuesto a una elevada interferencia, la PER en estos casos sería de hasta 45.6% y en el caso de que el coordinador ZigBee estuviese a menos de 2 metros del AP Wi-Fi, la PER podría llegar incluso al 100%. (Yang and Yu, 2008).

Por otro lado, si se transmitiera en los canales no solapados, la interferencia sería nula para el caso de la norma 802.11b y para el caso del 802.11g la PER podría ser de un 1.6% dependiendo del desplazamiento en frecuencia que exista entre un canal Wi-Fi y el canal ZigBee adyacente a este.

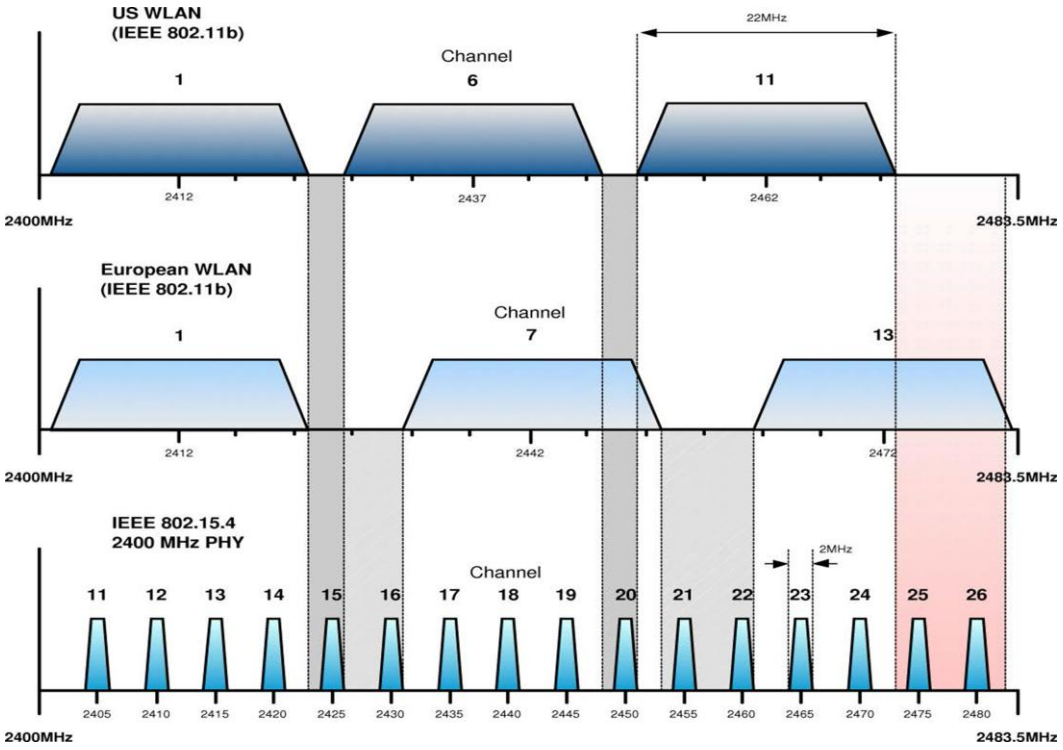


Figura 2.1: Canales de WLAN y ZigBee. (NXP Laboratories, 2013).

Para darle solución a este clásico problema, en este trabajo se utilizarán los canales 1, 6 y 11 de WLAN y el canal 26 de ZigBee, además el Coordinador ZigBee se colocará a más de 3 metros de cualquiera de los Access Point. Bajo estas condiciones se modificarán los atributos de cada uno de los dispositivos, tanto WLAN como ZigBee implementados en la red.

2. 3. Caracterización de la red a diseñar

Para una futura implementación de la red a diseñar se ha propuesto utilizar como ejemplo la Facultad de Ingeniería Eléctrica de la Universidad “Marta Abreu” de Las Villas, dependencia universitaria que tiene como propósito general ofrecer servicios docentes a estudiantes de varias carreras como Ingeniería Eléctrica, Ingeniería Biomédica, Ingeniería Automática e Ingeniería en Telecomunicaciones y Electrónica tanto del curso diurno como por encuentro, además como impartición de diplomados y postgrados. Dentro de esta se encuentran varias instituciones de investigación que apoyan el desarrollo docente de los

estudiantes, como el CEETI, el GARP y el CEDAI, vitales para la formación del ingeniero. (Iturria and Iglesias, 2013).

Este edificio mide 90m de largo y 12 metros de ancho y consta de 4 pisos. Para proveerle una confiable seguridad a esta instalación se ha propuesto utilizar el clásico equipamiento que se utiliza mundialmente para la vigilancia de edificios, así sean comerciales, empresariales o docentes, (esto es denominado mundialmente como Buildings Surveillance and Automation), este equipamiento se resume en sensores detectores de humo y calor (Smoke and Heat Detector), sensores detectores de movimiento (Motion Detector) y cámaras inalámbricas de alta resolución; también existen otra gran cantidad de dispositivos de vigilancia como sensores de gas, detectores de cristales rotos y sensores magnéticos, pero no se utilizarán en esta edificación. En la siguiente sección se realizará una descripción general de cada dispositivo utilizado y para mayores detalles consulte las hojas de especificaciones del fabricante en el Anexo II. El despliegue de cada equipo se ha realizado de la siguiente forma:

- **Primer Piso (Figura 2.2):** Aquí se encuentra ubicado el Router Central de la Facultad de Ingeniería Eléctrica, al cual están conectados 3 Switches ubicados en locales diferentes, distanciados aproximadamente unos 30m.
  - **Wi-Fi:** Cada uno de estos Switches tiene conectado un Access Point; esto se hace con el fin de lograr una mayor área de cobertura. Estos AP operan en los canales 1 y 6 (2 APs y 1 AP respectivamente) y tienen en permanente conexión a ellos 18 cámaras IP y un número relativamente alto de clientes Wi-Fi. Las cámaras están programadas para filmar sucesos cuando éstas detecten movimiento, y transmitir en tiempo real hacia su correspondiente AP a una razón de bit de 1200 Kbits/s. Por otro lado, los demás dispositivos Wi-Fi (laptops y/o smartphones) están configurados a que utilicen las aplicaciones HTTP, Email y FTP con un nivel de prioridad por debajo del asignado a las cámaras. Estas propiedades son asignadas de la misma manera a los demás dispositivos Wi-Fi en los restantes pisos.
  - **ZigBee:** Aquí se encuentra desplegado el Coordinador ZigBee, junto con 5 Routers, 30 Sensores detectores de humo y la sirena capaz de dar la alarma.

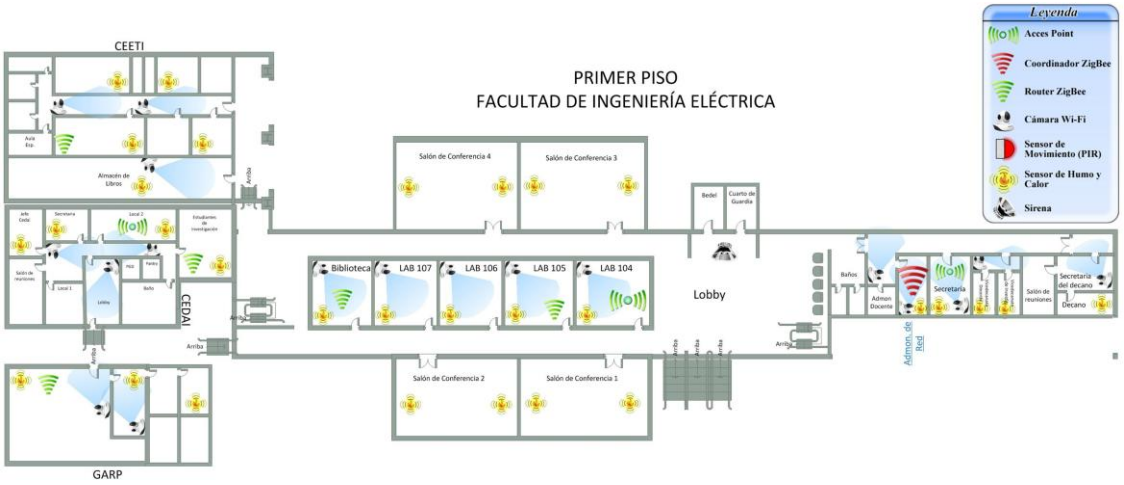


Figura 2.2: Estructura de la primera planta y ubicación de los equipos.

- **Segundo Piso (Figura 2.3):** Esta planta es conformada en su mayoría por laboratorios de investigación y departamentos de profesores, existe una fuerte red cableada, lo que hace menor la posibilidad de que algún usuario se conecte a la red Wi-Fi.
  - **Wi-Fi:** En esta planta se encuentran desplegados 2 APs, ambos operando en el canal 11, que dan cobertura a un total de 14 cámaras y que no interfieren en la banda de frecuencia de la primera planta.
  - **ZigBee:** Aquí se ubican 3 Routers, 15 Sensores de humo y 12 Sensores de movimiento.

Figura 2.3: Estructura de la segunda planta y ubicación de los equipos.

- **Tercer Piso (Figura 2.4):** Todo lo contario a la anterior, esta tercera planta está formada casi completamente por aulas y muy pocos departamentos de profesores,

por lo que se hace muy común que exista un mayor número de usuarios conectados a la WLAN.

- **Wi-Fi:** Debido a que las aulas requieren un nivel más bajo de seguridad respecto a otros locales, en esta planta solo se ubica 1 AP, operando en el canal 1 y dando conexión a 2 cámaras y a un número mayor de usuarios.
- **ZigBee:** Como ya se ha mencionado, en esta planta no es necesario un sistema de seguridad tan elevado con respecto a los dos primeros pisos. En este caso solo se utilizan 1 Router, 2 Sensores de humo y 1 Sensor de movimiento.

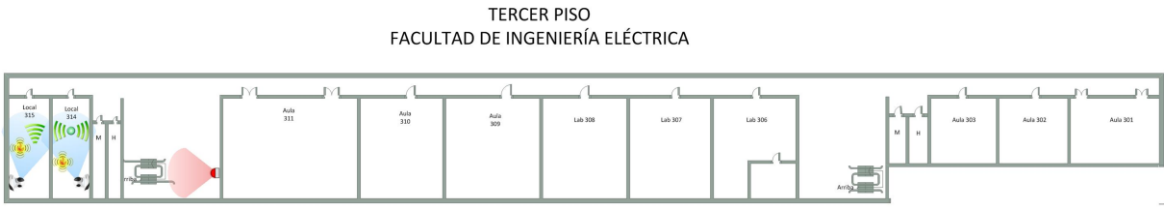


Figura 2.4: Estructura de la tercera planta y ubicación de los equipos.

- **Cuarto Piso (Figura 2.5):** Este caso es muy similar al anterior en cuanto a su estructura física y al nivel de seguridad que esta requiere.
  - **Wi-Fi:** Aquí se ubican 2 APs, operando ambos en el canal 6 y conectados a éstos, 3 cámaras y un número relativamente elevado de usuarios.
  - **ZigBee:** Solo es necesario utilizar 2 Routers, 3 Sensores de humo y 2 Sensores de movimiento.

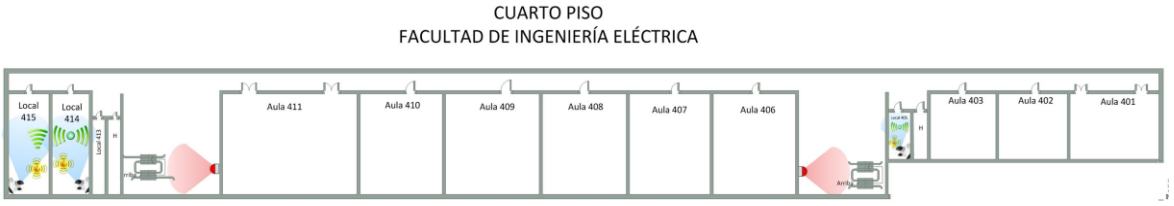


Figura 2.5: Estructura de la cuarta planta y ubicación de los equipos.

Luego de haber analizado la distribución física de cada uno de los dispositivos dentro de la edificación, se puede apreciar cómo se cuenta con un número fijo de 123 equipos, entre Wi-Fi y ZigBee, (la cantidad de usuarios conectados a la WLAN no se tiene en cuenta ya que

puede variar considerablemente en el transcurso del tiempo, además de que los datos que éstos envían tienen una prioridad inferior a la de las cámaras), los cuales se dividen en:

- **Wi-Fi:** 8 Access Point y 37 Cámaras Inalámbricas.
- **ZigBee:** 1 Coordinador, 11 Routers, 50 Sensores de humo, 15 Sensores de movimiento y la sirena de alarma.

Hay que resaltar aún un aspecto muy importante y es que cada uno de estos dispositivos son desplegados basándose en la infraestructura de red ya existente en esta instalación, o sea, que equipos como los Access Point serán conectados a los Switches que existen realmente en ese edificio.

2. 4. Selección del Hardware

Hoy en día, en el mercado mundial existen infinidad de fabricantes de equipos de vigilancia tanto de edificios como del hogar. Para la estructura de red propuesta en este trabajo se han seleccionado los equipos sensores fabricados por la Compañía N-R de Taiwán, los cuales son de fácil adquisición en el mercado y son relativamente baratos y de buena calidad con respecto a otras series de fabricantes, además poseen algunas características que resultan beneficiosas para este tipo de red como es el caso de que soportan topología árbol y malla, operan en la banda ISM de 2.4Ghz, se pueden alimentar tanto de la red eléctrica como de baterías y el coordinador ZigBee posee una fácil instalación a la red Ethernet; estos equipos mencionados utilizan el estándar ZigBee para su comunicación, los dispositivos que utilizan Wi-Fi (Access Point y cámaras) no pertenecen al mismo fabricante aunque no presentan problemas de compatibilidad entre ellos. Una descripción general de estos dispositivos se muestra a continuación:

- **Coordinator ZigBee mediante Ethernet (WZB-05ET):** Este es el dispositivo central que permite la conexión entre la red ZigBee de sensores y la red Ethernet, permitiendo el control y monitoreo de la misma al personal autorizado. Este dispositivo es muy utilizado en el control y la vigilancia de edificios y hogares, así como también en las aplicaciones industriales ya que funciona además como coordinador de sensores de temperatura, aceleración, vibración, velocidad de rotación, torque, entre otras magnitudes físicas. También existen otras versiones de

este dispositivo que permiten el control de la red ZigBee mediante puerto USB (WZB-01USBC), puerto RS485 (WZB-02485C) y Wi-Fi (G07-W).

- **Router ZigBee o Repetidor mediante USB (WZB-01USBR):** Este dispositivo permite le interconexión entre los sensores y el coordinador u otros routers, por lo que se utiliza como repetidor con el objetivo de ampliar el área de comunicaciones. Soporta topologías de malla y árbol y un máximo de 31 sensores conectados a él. Otra variante de este dispositivo es mediante puerto RS485 (WZB-02485R).
- **Sensor detector de humo y calor (WZB-SMT750):** Este sensor permite la detección de humo y/o oleadas de calor de hasta los 57°C mediante diodos infrarrojos. Puede ser programado para que envíe señales de aviso hacia el coordinador y/o puede él mismo activar una alarma sonora. Presenta además, una fácil instalación física así como una amplia compatibilidad con los routers ZigBee, haciendo posible el despliegue de estos sensores en edificaciones de gran tamaño.
- **Sensor detector de movimiento (WZB-SPM02):** Este sensor es similar al anterior, solo que su función es la de detectar movimiento utilizando infrarrojos pasivos (PIR), infrarrojos activos (AIR) y microondas (MW). Puede detectar personal no autorizado hasta unos 12 metros y permite además enviar un mensaje de aviso al coordinador si presenta algún mal comportamiento en su estructura interna.
- **Sirena de Alarma (A10):** Este dispositivo es de fácil instalación, recibe una señal de alerta y lanza un sonido de alarma de hasta 110db.
- **Access Point 802.11n (TP-LINK TL-WA901ND):** Este AP soporta velocidades de hasta 300Mbps, lo hace ideal para consumir ancho de banda o aplicaciones sensibles como el vídeo streaming, juegos en línea y VoIP. Soporta múltiples modos de funcionamiento (punto de acceso, Cliente, Universal / Repetidor WDS, Wireless Bridge). Posee una fácil configuración de encriptación WPA y amplia compatibilidad con los estándares IEEE 802.11b/g.
- **Cámara inalámbrica IP (Vstarcam):** Ésta cámara posee una fácil instalación física, tiene la capacidad de grabar video a alta resolución cuando detecta movimiento y enviar los datos en tiempo real hacia el Access Point y/o grabar el

video en una tarjeta SD. Trabaja bajo los estándares IEEE 802.11b/g/n. Puede configurarse fácilmente mediante los protocolos TCP/IP y HTTP y posee encriptación WEP/WPA-PSK/WPA2-PSK de 64/128bits.

La Hoja de Especificaciones de cada dispositivo aparece más detalladamente en el Anexo II. A continuación se presentan en la Tabla 2.1 los precios de cada equipo y el costo total de la red propuesta.

Dispostitivo	Cantidad	Precio C/U	Precio total
Coordinator ZigBee / Ethernet (WZB-05ET)	1	$105.00	$105.00
Router ZigBee USB (WZB-01USBR)	11	$95.00	$1045.00
Sensor detector de humo y calor (WZB-SMT750)	50	$49.00	$2450.00
Sensor detector de movimiento (WZB-SPM02)	15	$75.00	$1125.00
Sirena de Alarma (A10)	1	$55.00	$55.00
Access Point 802.11n (TP-LINK TL-WA901ND)	8	$55.00	$440.00
Cámara inalámbrica IP (Vstarcam)	37	$100.00	$3700.00
Total	123		$8920.00

Tabla 2.1: Precio de cada uno de los equipos a utilizar y coste total de la inversión.

2. 5. Conclusiones del capítulo

Luego de haber realizado el diseño de una red de vigilancia mediante sensores inalámbricos se ha podido concluir que:

- Ambos estándares (ZigBee y Wi-Fi) presentan problemas de interferencia en la banda de 2.4Ghz, pero otorgándole a Wi-Fi los canales 1,6 y 11 y a ZigBee el canal 26, se puede lograr una excelente compatibilidad entre ellos.
- Una red de sensores de este tipo puede tener un coste económico alto, pero es una inversión menor si se tiene en cuenta que su implementación ahorraría un capital más elevado para cualquier entidad universitaria, debido al hurto de sus medios materiales.

Capítulo III: Análisis del Desempeño de la Red WSN

En este capítulo se realiza la evaluación del comportamiento de una red WSN diseñada para un edificio docente. Para ello se utiliza la herramienta de Modelación y Simulación OPNET Modeler 14.5, evaluándose la carga, el retardo, la razón de transferencia y el tráfico para cada nodo.

3. 1. Herramienta OPNET Modeler

OPNET (Optimized Network Engineering Tools) Technologies, Inc. es un proveedor líder de soluciones para la gestión del rendimiento de aplicaciones y redes. Ofrece la mejor solución para: la gestión del rendimiento de aplicaciones, la gestión del rendimiento de la red y la red I+D. Ofrece una amplia visibilidad y control entre dominios de infraestructura, así como la recopilación de datos y análisis profundo para poder hacer un diagnóstico poderoso sobre la raíz del problema.

La compañía fue fundada en 1986 y comenzó a cotizar en el año 2000. Su sede reside en Bethesda, Marylan, y cuenta con oficinas en Cary, Carolina del Norte, Nashua, New Hampshire, Dallas, Texas y santa Clara, California. Cuenta con oficinas internacionales en Slough, Reino Unido, Paris, Francia; Gante, Bélgica; Frankfurt, Alemania y Singapur con el personal y los consultores en múltiples lugares en Asia y América Latina. El 29 de Octubre de 2012 fue adquirida por la tecnología Riverbed (Kanashiro, 2013).

Entre los distintos productos que OPNET posee se encuentra OPNET Modeler para el modelado y simulación. OPNET Modeler es un simulador basado en eventos orientado a la simulación de redes de telecomunicaciones. Para ser más explícitos lo podríamos definir como un simulador dinámico y discreto que puede realizar simulaciones deterministas y/o aleatorias basándose en teorías de redes de colas.

- Dinámico porque la representación del sistema durante la simulación evoluciona con el tiempo.

- Discreto porque el comportamiento de los sistemas representados cambia únicamente en instantes de tiempo concretos, es decir, eventos.
- Una simulación es aleatoria cuando durante la simulación entran en juego variables aleatorias. En cambio, se define como determinista cuando no entra en juego ninguna variable aleatoria. En OPNET se puede definir gran cantidad de variables y asignarles un patrón determinista o aleatorio.

OPNET Modeler es uno de los simuladores más avanzados en el campo de las redes de telecomunicaciones (Kanashiro, 2013).

3. 2. Análisis del Escenario de la Facultad de Ingeniería Eléctrica

Mediante la herramienta OPNET Modeler se ha realizado, en un solo escenario y los más exacto posible, el diseño de la red expuesta en el capítulo anterior. En la Figura 3.1 se puede apreciar más detalladamente el escenario de simulación en OPNET. Se ha hecho uso en este escenario de las tecnologías Wireless LAN y ZigBee, aplicando ambas dentro del mismo terreno de operación, con el objetivo fundamental de analizar su comportamiento en la banda de 2.4Ghz (banda común para ambas tecnologías) como ya se ha explicado en la Sección 2.2.

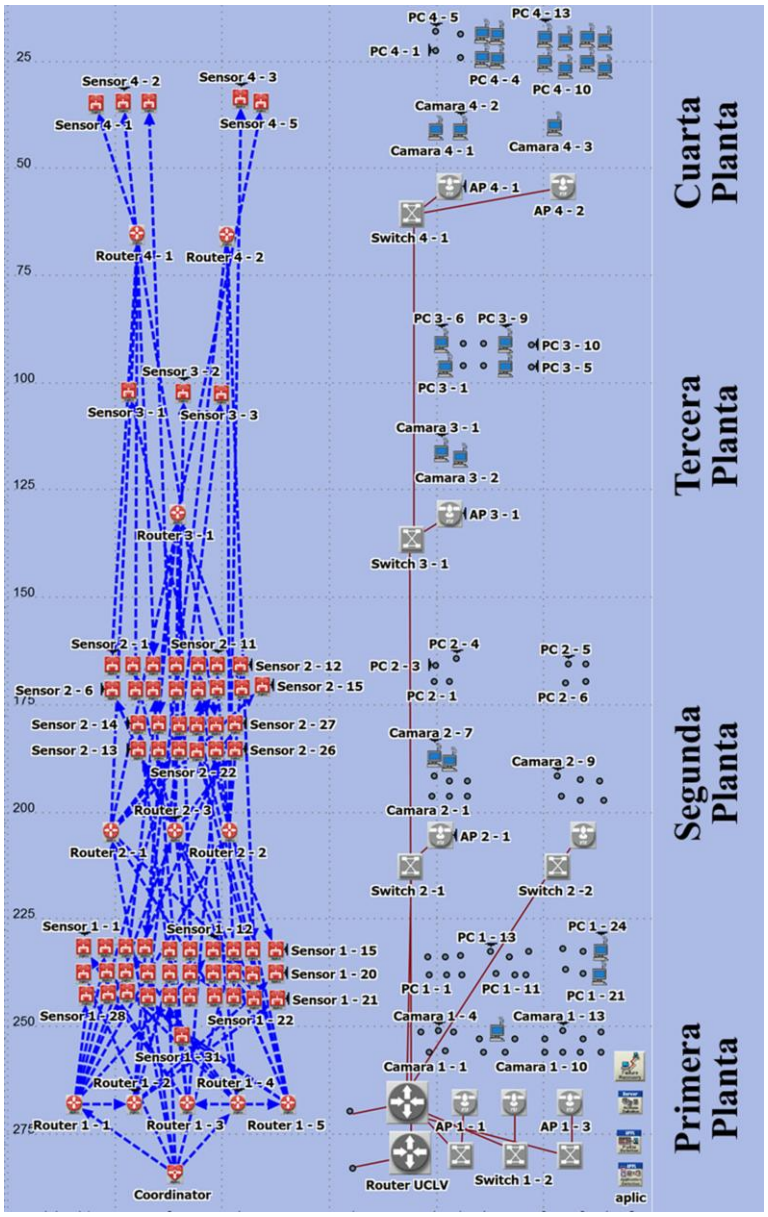


Figura 3.1: Modelo de simulación en OPNET Modeler de la red propuesta.

Como bien se observa en la figura, se ha hecho un despliegue de los dispositivos en cada piso, basándose en el plano físico (Sección 2.3) de dicha instalación universitaria, pudiéndose distinguir claramente las redes ZigBee y WLAN.

3. 2. 1. Arquitectura ZigBee

Para el despliegue de los dispositivos ZigBee se hizo uso de la Paleta de Objetos insertándose: 1 Coordinador, 11 Enrutadores o Repetidores (Routers) y 66 Dispositivos Terminales (End Devices). Cada uno de estos componentes tienen atributos en común como la banda de frecuencia a utilizar, el tamaño y destino de los paquetes y el tiempo de arribo de cada paquete. La configuración de cada atributo de los Dispositivos Terminales se puede observar más detalladamente en la Figura 3.2, estos atributos son los mismos, como se ha mencionado ya, que los utilizados para los Enrutadores.

Attribute	Value
name	Sensor 1 - 24
ZigBee Parameters	
MAC Parameters	
ACK Mechanism	(...)
Status	Enabled
ACK Wait Duration (seconds)	0.05
Number of Retransmissions	5
CSMA-CA Parameters	(...)
Minimum Backoff Exponent	3
Maximum Number of Backoffs	4
Channel Sensing Duration	0.25
Physical Layer Parameters	
Data Rate	250000
Packet Reception-Power Threshold	-85
Transmission Bands	(...)
2450 MHz Band	Enabled
915 MHz Band	Disabled
868 MHz Band	Disabled
Transmit Power	0.001
Device Type	End Device
PAN ID	1
Application Traffic	
Destination	Coordinator
Packet Interarrival Time	constant (300)
Packet Size	constant (500)
Start Time	constant (60)
Stop Time	Infinity

Figura 3.2: Configuración de los nodos de la red ZigBee.

Hay que señalar, que en la configuración de estos equipos solo varía el tiempo inicial (Start Time) con que se envía cada paquete: a los dispositivos de la primera planta se les ha asignado un valor de 60s y los demás dispositivos comienzan desfasados otros 60s por cada planta, o sea, 120s, 180s y 240s para la segunda, tercera y cuarta planta respectivamente. Esto se hace con el objetivo de evitar una congestión innecesaria en la red, además de lograr un mejor control y monitoreo de la misma.

Por otro lado, la configuración del nodo Coordinador solo difiere en que este dispositivo es el encargado de estructurar la red, por lo tanto posee atributos diferentes como bien se observa en la Figura 3.3. Este dispositivo es el que forma la topología de la red dependiendo de los valores que se le asignen en el campo "Parámetros de Red". Este aspecto difiere con respecto a una red WLAN en que el usuario no puede conectar directamente un dispositivo terminal con el coordinador, ni siquiera puede predecir cual sería la topología exacta resultante. En una red ZigBee los dispositivos se interconectan entre ellos mediante el procedimiento analizado en la sección 1.5.

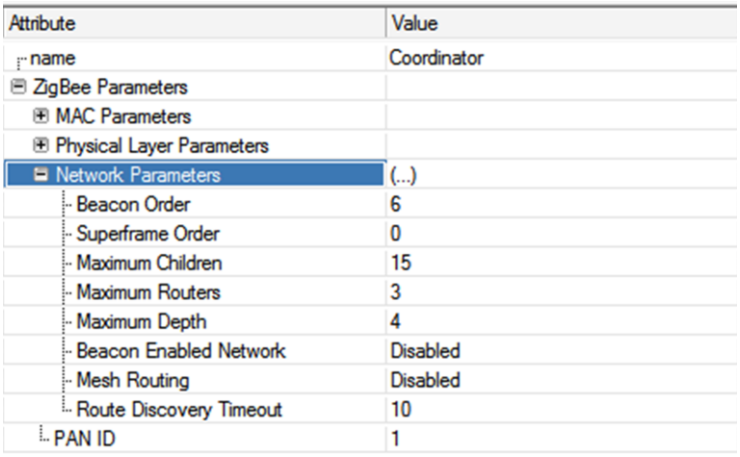


Figura 3.3: Configuración del Coordinador ZigBee.

La configuración de estos equipos resulta relativamente más fácil que en el caso de una red LAN típica o una WLAN, ya que para una red ZigBee no se tienen en cuenta algunos objetos que brinda OPNET como es el caso de los Perfiles y las Aplicaciones. En una red ZigBee los nodos se interconectan y forman la topología de la red de acuerdo a los valores establecidos por el Coordinador (Figura 3.3).

3. 2. 2. Arquitectura WLAN

Para el caso del diseño de la red WLAN, se han utilizado como componentes fundamentales 89 Estaciones de Trabajo (Workstations) inalámbricas, de ellas 37 haciendo función de cámaras y 52 haciendo función de equipos personales (Laptops y/o smartphones) y 8 Access Point conectados en base a la infraestructura de red existente en la instalación (Switches, Routers y Servidores) como se mencionó anteriormente y de la

forma que se observó en la Figura 3.1. Además se ha hecho uso de los componentes Perfiles y Aplicaciones.

La primera planta cuenta con la instalación de tres Access Point ya que hay gran cantidad de locales de trabajo y por consiguiente mayor cantidad de cámaras de vigilancia, además hay un mayor número de usuarios conectados a la red WLAN con respecto a las demás plantas de la instalación. Dos de estos Access Point operan bajo el canal 1 de la banda de 2.4Ghz y el restante Access Point opera bajo el canal 6, logrando así un mejor dominio del espectro de frecuencias. En la segunda planta se han instalado dos Access Point operando ambos bajo el canal 11. En las plantas restantes, los Access Point operan bajo los canales 1 y 6, tercera y cuarta planta respectivamente. Todos estos Access Point trabajan bajo el estándar IEEE 802.11g.

En esta simulación se han utilizado cuatro aplicaciones denominadas: Video, Email, Ftp y Http. En el caso de la aplicación “Video” se ha configurado para que toda la información sea enviada desde la cámara de vigilancia hacia el servidor de la facultad FIE a una razón constante de unos 1200 Kbits/s (150 Kbytes/s), ésta razón de transmisión garantiza una relativamente alta calidad de video. Para el caso de las restantes aplicaciones, se han establecido todas bajo el valor de Alta Carga (High Load), con el objetivo de simular un caso crítico donde todos los usuarios estén haciendo máximo uso de la red.

Basándose en estas cuatro aplicaciones se han definido dos perfiles, denominados “Cámara” y “Usuarios”. El primero de estos utiliza 5 aplicaciones “Video”, todas ellas configuradas con una duración entre 2 – 4 minutos y con una repetición del suceso de 28 – 32 minutos y estas aplicaciones están desfasadas unas de otras 100s con el objetivo de simular un caso crítico en el que todas las cámaras estén transmitiendo casi simultáneamente. El otro perfil denominado “Usuarios” contiene las aplicaciones Http, Ftp y Email. Utilizando estos dos perfiles trabajan los dispositivos desplegados en la simulación, las cámaras y el Servidor FIE utilizan el perfil “Cámara” y los equipos personales junto al Servidor UCLV utilizan el perfil “Usuarios”.

3. 3. Análisis de los Resultados

Basándose en la previa estructura de red ya expuesta, en esta sección se realizará un análisis de los resultados de dicha red en un intervalo de tiempo de simulación de una hora mediante gráficas y tablas facilitadas por OPNET.

3. 3. 1. Resultados ZigBee

El primer aspecto a tratar es la topología de red resultante en la arquitectura ZigBee (Figura 3.1 izquierda), la cual se formó a partir de las configuraciones hechas en el coordinador de la red (Figura 3.3). Se debe recordar que esta topología nunca es absoluta, puede variar en respuesta a determinados eventos que ocurran en el entorno, por ejemplo un mal funcionamiento de cualquiera de los Repetidores o una baja recepción de la señal, hace que los nodos Terminales busquen un camino alternativo hacia el coordinador, por lo que cambiaría la topología de la red (Sección 1.5).

Otro aspecto importante a tratar es el flujo del tráfico en la red. En la Figura 3.4 se ve reflejado el flujo de paquetes generados por la capa de aplicación de un nodo sensor; otras estadísticas como el tráfico enviado por la subcapa MAC, el número de intentos de retransmisión de paquetes y el delay se muestran en el Anexo III. Estos resultados son una ratificación de lo antes expuesto en la configuración de cada nodo sensor: el tamaño de cada uno de estos paquetes es de 500 bits y el tiempo de arribo de éstos es de 5 minutos, ver Figura 3.2.

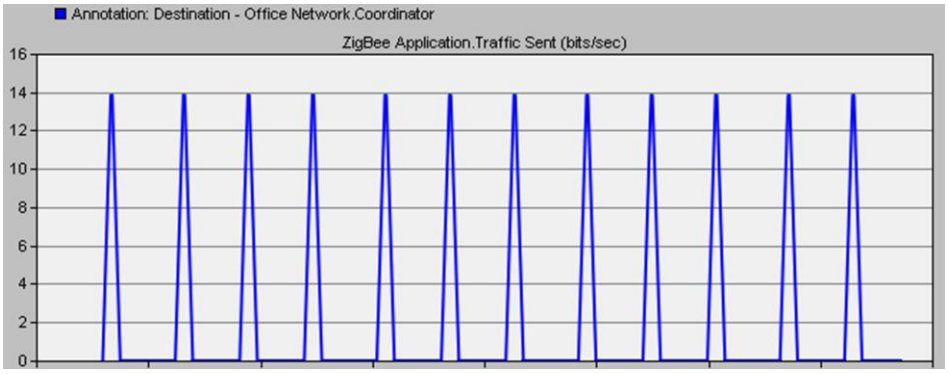


Figura 3.4: Tráfico enviado por la capa de aplicación de un nodo sensor.

Por otro lado, hay que analizar el tráfico que llega hasta la capa de aplicación del nodo coordinador. En la Figura 3.5 se puede evidenciar en la gráfica como el coordinador recolecta toda la información enviada por los nodos sensores y repetidores. La diversidad en las amplitudes en las curvas se debe a que como anteriormente se expuso, los nodos sensores están desfasados 60 segundos por cada piso.

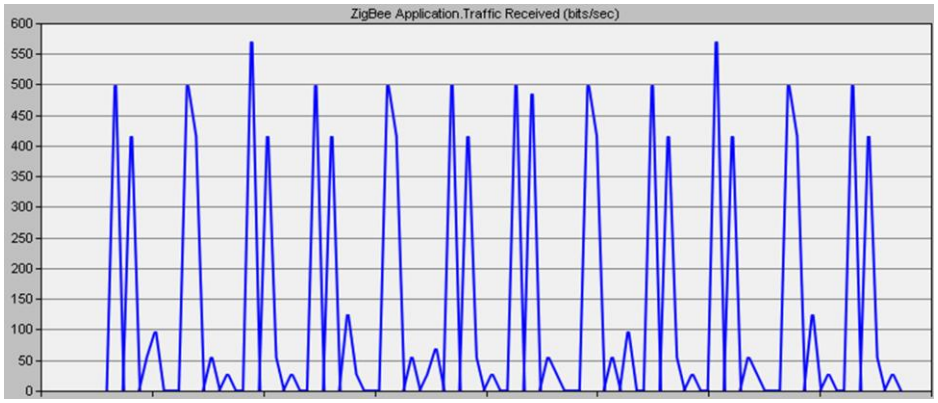


Figura 3.5: Tráfico recibido por la capa de aplicación del coordinador.

La Figura 3.6 consiste en un gráfico integrador de la cantidad de paquetes por segundo que recibe el coordinador, como se puede apreciar, cada 5 minutos el coordinador recibe con plenitud los 77 paquetes enviados por cada uno de los sensores y repetidores.

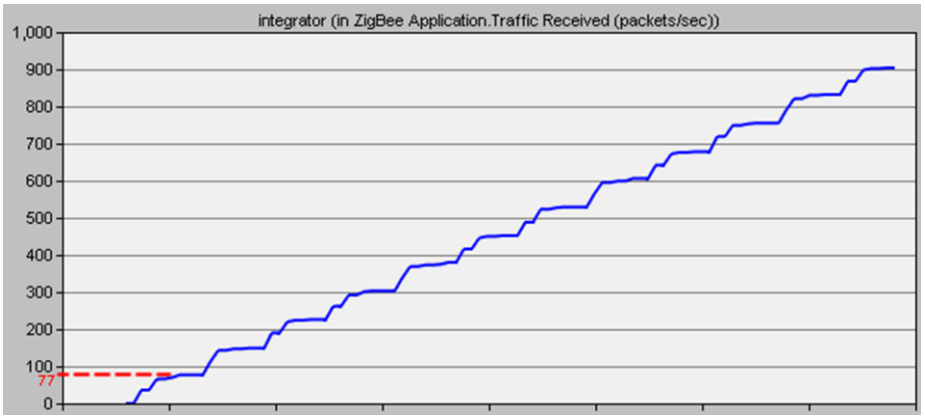


Figura 3.6: Tráfico total recibido por la capa de aplicación del coordinador.

3. 3. 2. Resultados WLAN

El análisis de los resultados de la red WLAN está enfocado principalmente en el desempeño de las cámaras, el tráfico que éstas generan y el retardo que presentan para la

red. Se analizará además, pero en menor escala el tráfico que generan las aplicaciones utilizadas por los usuarios que son Http, Email y FTP, ya que como se ha mencionado anteriormente, la aplicación de Video utilizada por las cámaras posee un nivel de prioridad por encima del resto de las aplicaciones, además no constituye un objetivo específico en esta tesis el analizar el desempeño de estas aplicaciones.

El primer aspecto a analizar es el tráfico que envía y recibe una sola cámara hacia el servidor FIE mediante la aplicación de Video. Como bien se observa en la Figura 3.7 cada cámara envía a una razón constante de 150000 bytes/seg, y recibe a 500 bytes/seg también a una razón constante, por lo que bien pudiera hacerse una visualización en tiempo real de dicha grabación de Video. Por otro lado, en la Figura 3.8 se evidencia el bajo retardo (solo unos 7ms) que presentan dichas cámaras.

Figura 3.7: Tráfico enviado y recibido por la aplicación de Video de una cámara hacia el servidor FIE.

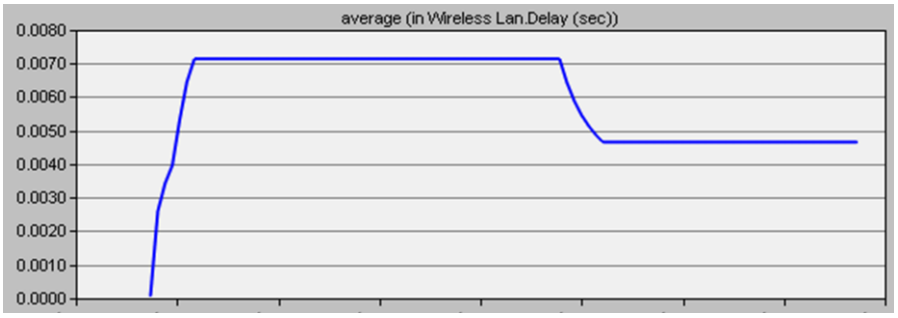


Figura 3.8: Retardo en la red de la aplicación de Video.

Hay que destacar además el comportamiento en la red de los Access Point, analizando algunas estadísticas como la razón de transferencia exitosa (throughput) y el retardo (delay), Figuras 3.9 y 3.10 respectivamente. Para ello se ha tomado como referencia el AP del primer piso que opera en el canal 6, ya que éste les posibilita la conexión a la red a 8 cámaras y 6 usuarios.

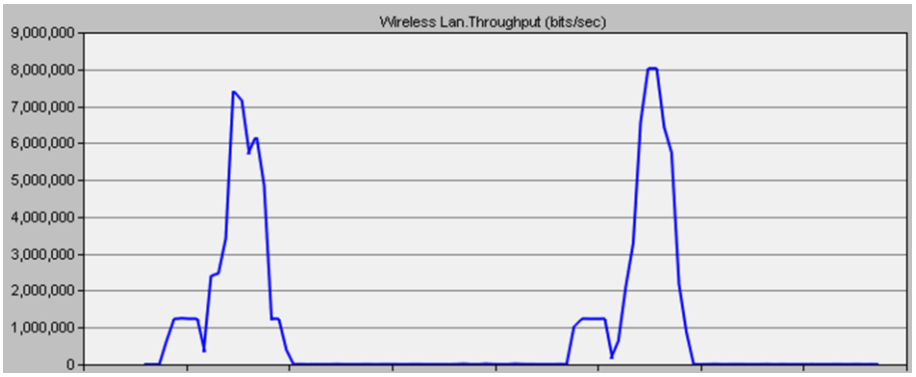


Figura 3.9: Razón de transferencia exitosa que presenta un Access Point.

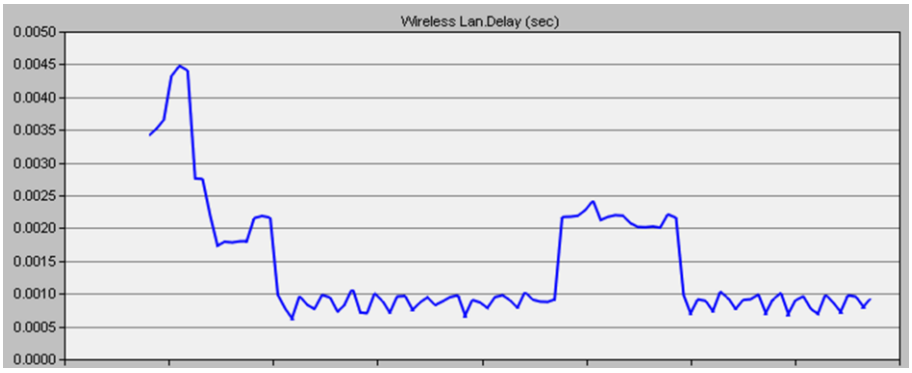


Figura 3.10: Retardo de un Access Point.

Este Access Point presenta una carga que alcanza niveles de hasta 300kbps como bien se evidencia en la Figura 3.11. Los valores picos que se observan en la imagen corresponden al tráfico enviado por la aplicación de Video, la cual prevalece por encima del resto de las aplicaciones. Caso similar a esto se pudo apreciar en la Figura 3.10, donde el retardo es mayor para la aplicación de Video.

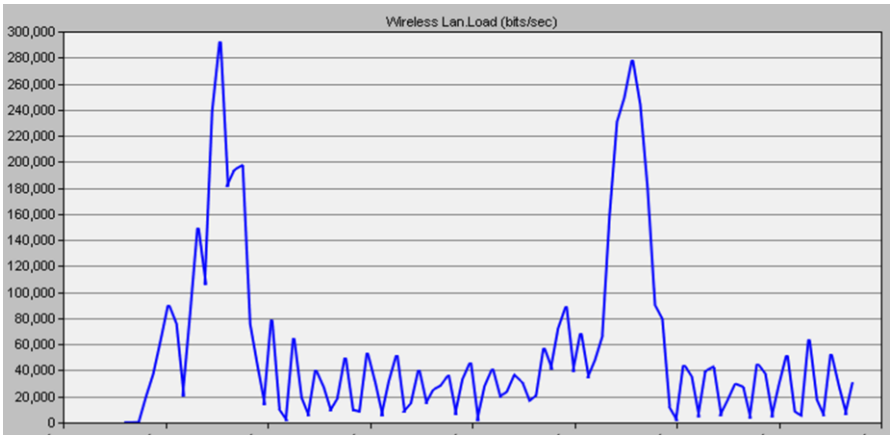


Figura 3.11: Comportamiento de la carga en la red de un Access Point.

Como último tema de este capítulo, se propone analizar el tráfico que recibe el servidor FIE mediante la aplicación de Video y comparar este resultado con el tráfico que recibe el servidor UCLV que administra las aplicaciones HTTP, FTP, Email. En la Figura 3.12 se puede apreciar el tráfico total recibido por el servidor FIE, este alcanza valores sobre los 20Mbits/s y el retardo en las zonas de mayor demanda no sobrepasa el milisegundo.

Figura 3.12: Tráfico recibido y retardo del servidor FIE.

Comparando estos valores para el caso del servidor UCLV, ver Figura 3.13, se puede apreciar como éste último recibe mucho menos tráfico pero en un intervalo de tiempo mayor. Mediante un gráfico integrador se observa la notable diferencia del tráfico total recibido por ambos servidores.

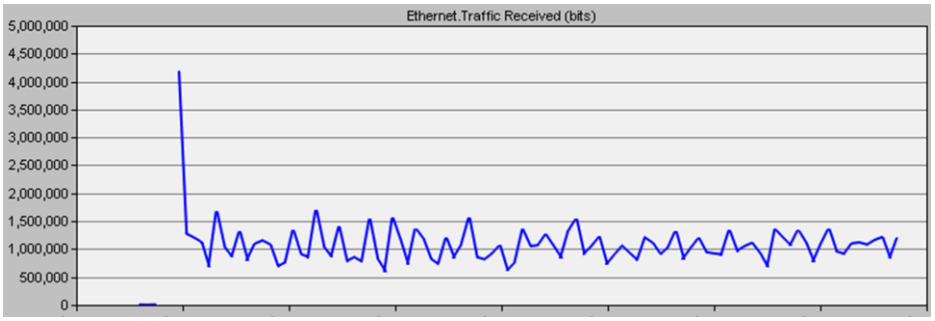


Figura 3.13: Tráfico recibido por el servidor UCLV.

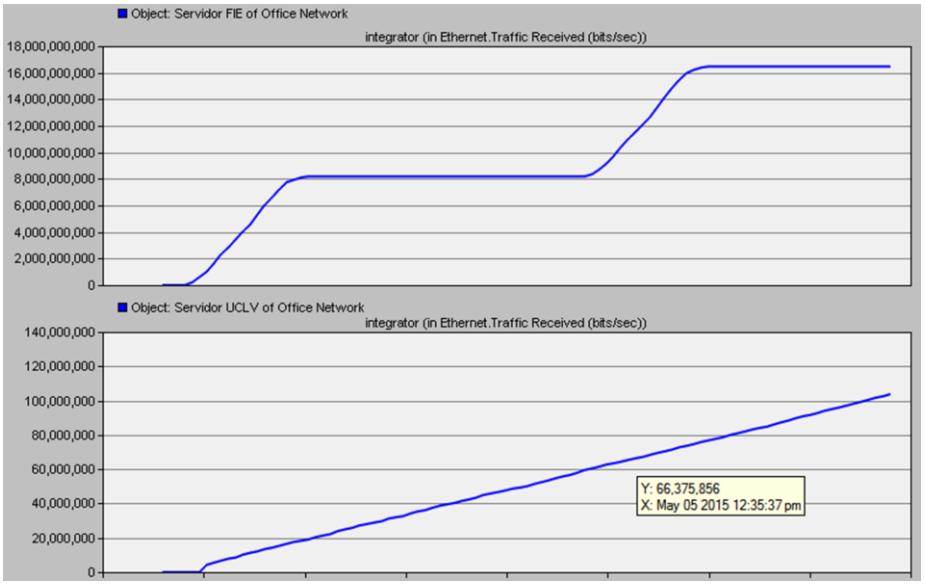


Figura 3.14: Gráfico integrador del tráfico total recibido por los servidores FIE y UCLV.

3. 4. Conclusiones del capítulo

Posterior al análisis de la simulación de la red diseñada se ha podido comprobar que:

- Se ha podido corroborar la afirmación del capítulo anterior, que ZigBee y Wi-Fi pueden emplearse de forma armónica en la Banda de 2.4GHz, empleando para ZigBee el canal 26, de forma que no interfiera con los canales 1,6 y 11 de Wi-Fi.
- El tráfico de video representa casi un 90 % del tráfico total, con una latencia de 7ms de los paquetes
- Debido al tiempo de respuesta del servidor FIE (150ms) y al retardo de los Access Point (5ms), pueden transmitir simultáneamente hasta 11 cámaras de video.

Conclusiones y Recomendaciones

Conclusiones

- Se ha evidenciado mediante síntesis bibliográfica y algunos ejemplos reales de aplicación que el estándar ZigBee sobresale sobre los demás estándares en cuanto a aplicaciones de vigilancia y combinando esta tecnología con Wi-Fi se puede lograr un sólido mecanismo de seguridad en edificios.
- Se ha logrado además, diseñar una propuesta de Red Inalámbrica de Sensores para aplicaciones de vigilancia utilizando ambas tecnologías, logrando una eficiente compatibilidad entre ellas y aprovechando al máximo sus beneficios.
- Mediante la herramienta de simulación y modelación OPNET se ha realizado un despliegue de la red diseñada con el objetivo de evaluar el comportamiento de ambas tecnologías y de demostrar que el tráfico generado por los dispositivos Wi-Fi de esta nueva red no afecta en un nivel significativo a el tráfico de los demás equipos existentes en la red como las laptops.

Recomendaciones

- Aplicar los procedimientos de diseño antes expuestos para implementar la red propuesta con el objetivo de lograr una mayor seguridad en la universidad.
- Fomentar en el programa académico existente el estudio teórico de las redes inalámbricas de sensores como parte de alguna asignatura afín de la facultad.
- Implementar, además del conocimiento teórico, la utilización de Herramientas de Modelación y Simulación para garantizar la preparación que exige la carrera.

Referencias Bibliográficas

6LOWPAN 2012. Ipv6 over IEEE 802.15.4.

AHMED, M. A. & KIM, Y.-C. 2013. Hybrid Communication Network Architectures for Monitoring Large-Scale Wind Turbine. Available: http://dx.doi.org/10.5370/JEET.2013.8.?.742.

ALIBABA GROUP. 2014. *Smart home automation* [Online]. Available: http://www.alibaba.com.

BLUETOOTH 2011.

CARBAJAL, E. E. F. 2012. *Redes de Sensores Inalámbricas Aplicado a la Medicina.* Universidad de Cantabria.

DARGIE, W. & POELLABAUER, C. 2010. Fundamentals of Wireless Sensor Networks. Theory and Practice.

DIGNANI, J. P. 2011. *Análisis del Protocolo ZigBee.* Universidad Nacional de La Plata.

DONG, W. 2010. Providing OS Support for Wireless Sensor Networks: Challenges and Approaches. *IEEE Communications Surveys & Tutorials* [Online].

FAROOQ M, T. K. 2011. Operating Systems for Wireless Sensor Networks: A Survey. Sensors.

GARCÍA-HERNANDO & MARTÍNEZ-ORTEGA. 2008. Problem Solving for Wireless Sensor Networks Computer Communications and Networks.

GASPARINI, L. 2010. *Ultra-low-power Wireless Camera Network Nodes. Design and Performance Analysis.*, University of Trento.

IEEE 1999a. Std 802.11a: High-speed Physical Layer in the 5 GHz Band.

IEEE 1999b. Std 802.11b: Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

IEEE 2003. Std 802.11g: Extended Rate Physical Layer in the 2.4 GHz Band.

IEEE 2009. Std 802.11n: Enhancements for Higher Throughput.

IEEE 2011. Std 802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *General Description.*

IEEE 2012. Std 802.11: Revision of IEEE Std 802.11-2007.

IEEE 2013. Std 802.11ac: Amendment to IEEE Std 802.11™-2012.

ITURRIA, P. & IGLESIAS, D. 2013. Proyecto de Red: Facultad de Ingeniería Eléctrica.

KANASHIRO, W. R. R. 2013. *Redes inalámbricas y simulación de WLAN mediante OPNET.* Universidad de Cataluña.

KARL, H. & WILLIG, A. 2005. Protocols and Architectures for Wireless Sensor Networks. *In:* LTD, J. W. S. (ed.).

KUORILEHTO, M., KOHVAKKA, M., SUHONEN, J., H¨AM¨AL¨AINEN, P., H¨ANNIK¨AINEN, M. & H¨AM¨AL¨AINEN, T. D. 2007. Ultra-Low Energy Wireless Sensor Networks in Practice. *In:* LTD, J. W. S. (ed.). Tampere University of Technology, Finland.

LINARES, J. M. 2014. *Simulación e implementación de una red de sensores inalámbrica multisalto para la medición de consumo energético en un edificio.*, Universidad Politécnica de Cataluña.

NAVARRO, J. 2010. *Simulación de Redes de Sensores Wireless.* Universidad Autónoma de Barcelona.

NXP LABORATORIES. 2013. Co-existence of IEEE 802.15.4 at 2.4 GHz. Available: http://www.nxp.com.

REDDY, A. 2009. Operating Systems for Wireless Sensor Networks: A Survey. *International Journal of Sensor Networks* [Online], 5.

SALVETTI, D. 2012. Redes Wi-Fi en entornos Windows.

WANG, Q. & BALASINGHAM, I. 2010. Wireless Sensor Networks - An Introduction.

WIRELESSHART 2009.

YANG, G. & YU, Y. 2008. *WLAN 802.11 b/g interference into ZigBee networks.* Agder University.

Z-WAVE ALLIANCE 2008.

ZIGBEE ALLIANCE 2011. ZigBee Specification Overview.

Anexos

Anexo I: Tipos de sensores utilizados en Redes de Sensores Inalámbricas.

	Sensor	Características
Temperatura	Sensor de temperatura electromecánico	Compuesto por termostatos de metal que reaccionan ante la contracción o expansión de materiales sometidos a cambios de temperatura.
	Sensor de temperatura eléctrico (termopares)	Compuesto por una pareja de metales que generan un flujo de corriente al existir una diferencia de temperatura.
	Sensor de Silicio	Utiliza la resistencia eléctrica masiva de materiales semiconductores.
	Sensor de temperatura resistivo (termistores)	Basa su funcionamiento en una resistencia que cambia conforme la temperatura.
	Detector de temperatura resistivo	Constituido completamente de metal, a diferencia de los termistores que incluyen cerámica. Cubre mayores rangos de temperatura.
Humedad	Sensor de humedad relativa capacitivo	Reacciona a la humedad relativa en el medio ambiente.
	Sensor de humedad resistivo	Utiliza el cambio de resistencia para medir la humedad, es pequeño y de bajo costo.
Químicos	Sensor de Transductor Interdigital	Formado por una capa que sirve como dieléctrico entre dos electrodos, cuyas propiedades cambian cuando interactúan con determinadas sustancias.
	Sensor de conductividad	Al interactuar con algunos productos químicos, la conductividad se modifica.

	Sensor óptico químico	A través de ondas ópticas se detectan reacciones químicas. En su mayoría son sensores de gas.
	Sensor químico piezoeléctrico	Utiliza el efecto piezoeléctrico, consistente en la generación de una carga eléctrica sobre un material. Responde a los cambios de composición química.
Mecánicos	Sensor de presión	Mide la presión, por ejemplo la presión de un líquido (barómetro)
	Sensor magnético de posición	Tiene la tarea de descubrir, medir intensidad, dirección, rotación o variación de un campo magnético.
	Sensor ultrasónico de posición	Similar a un radar, identifica objetivos a través de ondas de sonido de alta frecuencia.
	Acelerómetro	Mide la aceleración a la que es sometido, con este tipo de sensor es posible detectar actividades volcánicas, conocer la rigidez de una estructura o del cuerpo humano, como huesos y articulaciones.
Médicos	Oxímetro	Analiza la oxigenación de la sangre a través de la hemoglobina del paciente.
	Sensor de oxígeno	Mide la cantidad y proporción de oxígeno en la sangre.
	Sensor de flujo de sangre	Utiliza el desplazamiento Doppler de una onda ultrasónica para reflejarla en la sangre.
	ECG (electrocardiograma)	Mide la Frecuencia cardiaca
	EEG (electroencefalografía)	Analiza la actividad eléctrica del cerebro
	EMG (electromiografía)	Utilizado para medir la actividad muscular
	Sensor medidor de glucosa	Mide los niveles de glucosa presentes en la sangre

Otros	Sensor foto acústico	A través de espectroscopia puede detectar la presencia de gases. Sumamente utilizado para detectar fugas en las tuberías.
	Cilindro piezoeléctrico	Mide la velocidad de los gases.
	Sensor infrarrojo pasivo	Utiliza radiación infrarroja para detectar movimiento.
	Sensor sísmico	Mide las ondas símicas y vibraciones, utilizado para la detección y prevención de terremotos.
	Sensor de emisión acústica	Mide los cambios micro-estructurales o desplazamientos a través de las ondas que genera.

Anexo II: Hojas de Especificaciones de los dispositivos.

Coordinador ZigBee / Ethernet WZB-05ET

Protocolo de Transmisión	UART: Modbus RTU / ZigBee: HA profile
Protocolo Inalámbrico	Compliant IEEE 802.15.4, ZigBee2007/PRO
Chip-Set	TI ZigBee SoC CC2530F256, 256K Flash
Frecuencia de Operación	2.4GHz ISM
Canales	16
Rango de Transmisión	500m (exteriores), 80m (interiores)
Razón de Transmisión	250kbps Máx.
Potencia de Salida RF	18dBm
Sensibilidad del Receptor	-92dBm
Voltaje de Operación	DC 5V, adaptador USB
Consumo de Potencia	0.8W
Ganancia de la Antena	2dBi Omnidireccional
Topologías de Red	Estrella, Árbol y Malla

Protocolos de Red	ARP, IP, ICMP, UDP, TCP, HTTP, DHCP, Telnet
Razón de Datos	10/100Mbits/sec
Configuración de Parámetros	Vía Servidor Web
Configuración de Red	IP estático ó DHCP

Router ZigBee o Repetidor mediante USB WZB-01USBR

Protocolo de Transmisión	UART: Modbus RTU / ZigBee: HA profile
Protocolo Inalámbrico	IEEE802.15.4/ZigBee 2007/PRO
Chip-Set	TI/C2530F256, 256 Flash SoC
Potencia de Salida RF	18dBm
Sensibilidad del Receptor	-92dBm
Rango de Transmisión	500m (exteriores); 80m (interiores)
Razón de Transmisión	250kbps Máx.
Interfaz de Salida	USB
Parámetros Configurables	Baud rate, PAN ID, Canales RF
Topologías de Red	Estrella, Árbol y Malla
Auto reconexión	Sí
Sistemas operativos	Windows: 2000, XP, Vista, Win7, Win8

Sensor detector de humo y calor WZB-SMT750

Protocolos de Transmisión	UART: Modbus RTU / ZigBee: HA profile
Protocolo Inalámbrico	Compliant IEEE 802.15.4, ZigBee2007/PRO
Chip-Set	CC2530
Direccionamiento	IEEE MAC 64bit
Transmission Range	100m (exteriores); 30m (interiores)
Frecuencia de Operación	2.4GHz ISM

Potencia de Salida RF	0dBm
Sensibilidad del Receptor	-90dBm
Suministro de Energía	DC 9V~24V
Corriente en Reposo	55uA
Indicación de Alarma	LED Rojo
Corriente de Alarma	18mA @ 12V
Corriente Estática	55uA
Topologías de Red	Estrella, Árbol y Malla
Sistemas Operativos	Windows NT/2000/XP/Vista/ Win 7/8
Duración de la Batería	≈ 1 año
Auto reconexión	Sí

Sensor detector de movimiento WZB-SPM02

Protocolo de Transmisión	UART: Modbus RTU / ZigBee: HA profile
Protocolo Inalámbrico	Compliant IEEE 802.15.4, ZigBee2007/PRO
Modelo	SPM-02 Motion Detector
Método de Detección	Infrarrojo Pasivo, Infrarrojo Activo y Microondas
Chip-Set	TI C 2530F 256, 256K Flash SoC
Potencia de Salida RF	0 dBm
Rango de Transmisión	100m (exteriores); 30m (interiores)
Razón de Transmisión	250kbps Máx.
Sensor Microondas	X-Band Mono-static DRO
Frecuencia Microondas	10.525 GHz
Altura de Montaje	2m
Suministro de Energía	10~16V (12 VDC normal)
Rango de detección	12m
Indicador de Alarma	Pantalla LED
Auto reconexión	Sí

Sirena de Alarma A10

Protocolo de Transmisión	UART: Modbus RTU / ZigBee: HA profile
Protocolo Inalámbrico	Compliant IEEE 802.15.4, ZigBee2007/PRO
Chip-Set	TI ZigBee SoC CC2530F256, 256K Flash
Frecuencia de Operación	2.4GHz ISM
Rango de Transmisión	50m (exteriores); 15m (interiores)
Razón de Transmisión	250kbps Máx.
Potencia de Salida RF	4 dBm
Sensibilidad del Receptor	-92dBm
Suministro de Energía	DC 12V
Consumo de Potencia	0.8W Máx
Ganancia de la Antena	PCB Direccional
Topologías de Red	Estrella, Árbol y Malla
Auto reconexión	Sí

Access Point 802.11n TP-LINK TL-WA901ND

Protocolo Inalámbrico	IEEE 802.11b/g/n
Frecuencia de Operación	2.4GHz ISM
Razón de Transmisión	802.11n: Hasta 300Mbps (dinámico)
	802.11g: Hasta 54Mbps (dinámico)
	802.11b: Hasta 11Mbps (dinámico)
Potencia de Salida RF	20 dBm
Sensibilidad del Receptor	PER 270M:-68dBm @ 10%
	PER 130M:-68dBm @ 10%
	PER 54M:-68dBm @ 10%

	PER 11M:-85dBm @ 8%
	PER 6M:-88dBm @ 10%
	PER 1M:-90dBm @ 8%
Suministro de Energía	DC 12V
Modos Inalámbricos	Modo AP
	Multi-SSID Mode
	Modo Cliente AP
	Modo repetidor (WDS / Universal)
	AP + en modo Bridge (punto a punto o punto a multipunto)
Ganancia de la Antena	4dbi Omnidireccional x3
Modulación	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Interfaz Ethernet	10/100 Ethernet, Apoyo PoE

Cámara inalámbrica IP Vstarcam

Protocolo Inalámbrico	IEEE 802.11b/g/n
Frecuencia de Operación	2.4GHz ISM
Razón de Transmisión	802.11n: Hasta 150Mbps (dinámico)
	802.11g: Hasta 54Mbps (dinámico)
	802.11b: Hasta 11Mbps (dinámico)
Potencia de Salida RF	15 dBm
Sensibilidad del Receptor	150M:-68dBm@10%PER
	130M:-68dBm@10%PER
	108M: -68dBm@10% PER
	54M:-70dBm@10%PER
	11M:-88dBm@8%PER
	6M:-90dBm@10%PER
	1M:-92dBm@8%PER
Suministro de Energía	DC 5V

Ganancia de la Antena	2dbi SMA
Modulación	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Interfaz Ethernet	10/100 Ethernet
Seguridad Inalámbrica	64/128-bit WEP/WPA-PSK/WPA2-PSK
Protocolos de Red	TCP/IP, HTTP, SMTP, FTP, DHCP, DNS, DDNS, NTP, UPnP, PPPoE, P2P etc.
Formato Codificador de Video	H.264 baseline profile@levels:3.1/Motion-JPEG
Resolución	720p/VGA/QVGA
Razón de Bit de Video	128~4096kbps
Razón de Cuadros	30fps/24fps(720p)

Anexo III: Resultados secundarios de la simulación.

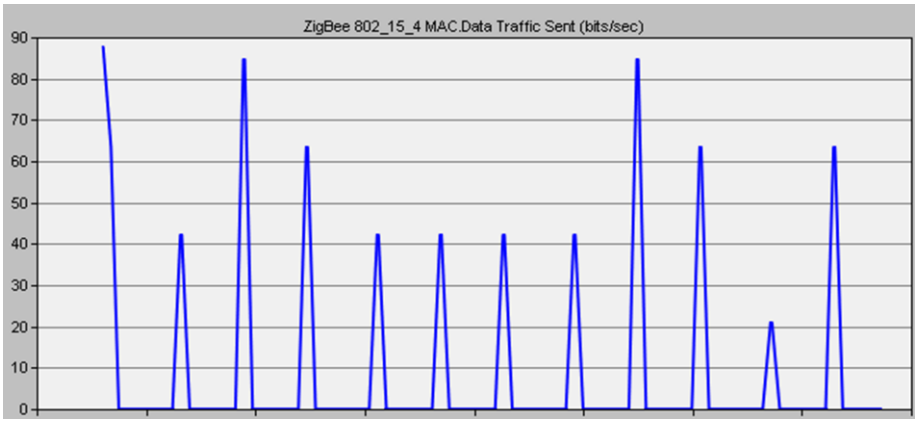


Figura A.1: Tráfico enviado por la subcapa MAC de un nodo sensor.

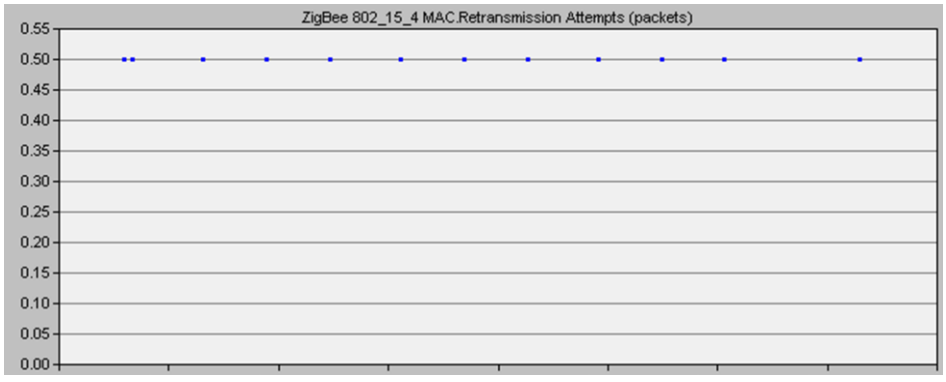


Figura A.2: Intentos de retransmisión de paquetes de un nodo sensor.

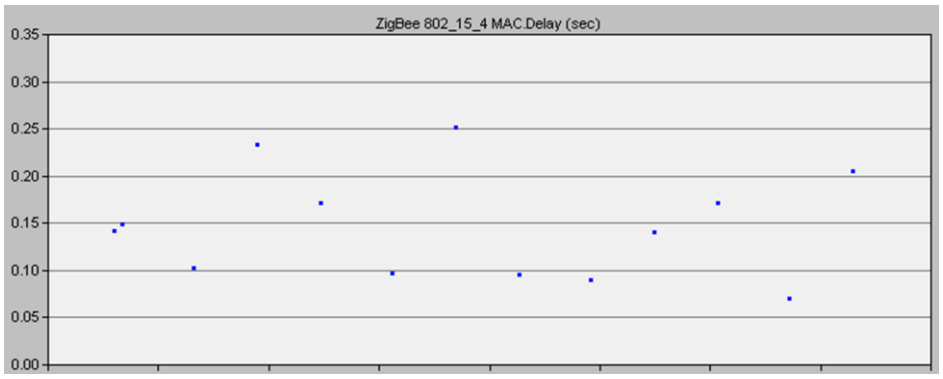


Figura A.3: Retardo de los paquetes de un nodo sensor.

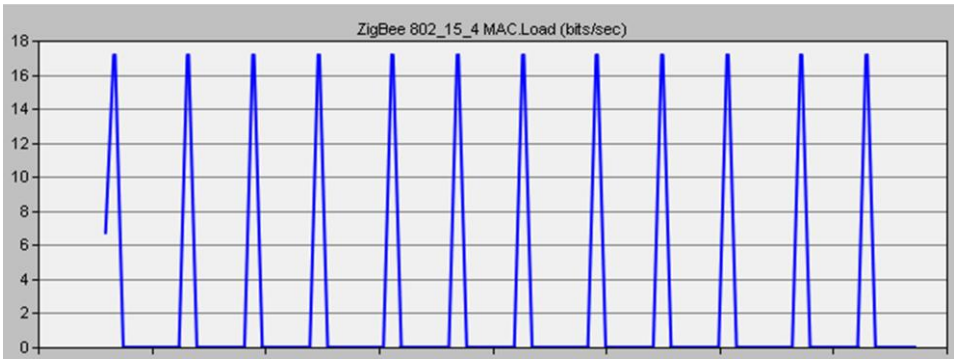


Figura A.4: Carga que presenta un nodo sensor.

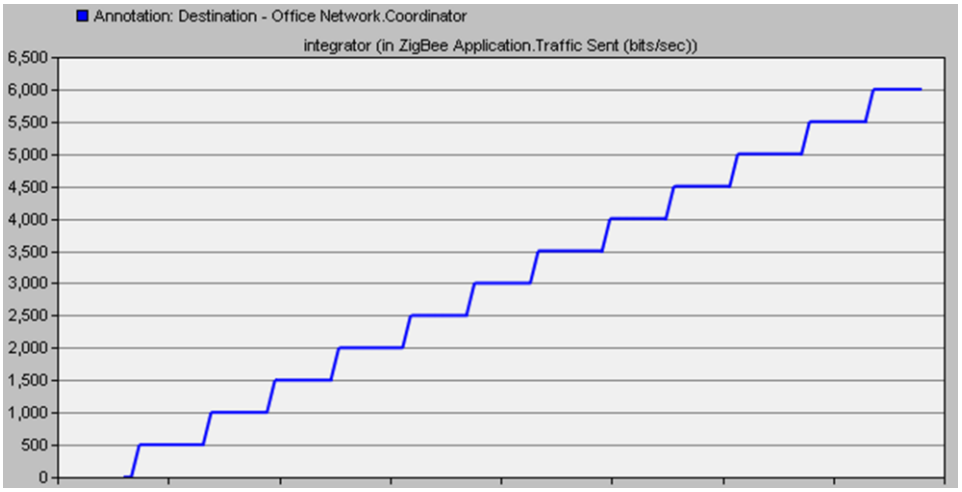


Figura A.5: Gráfico integrador de los paquetes enviados por la capa de aplicación un nodo sensor.

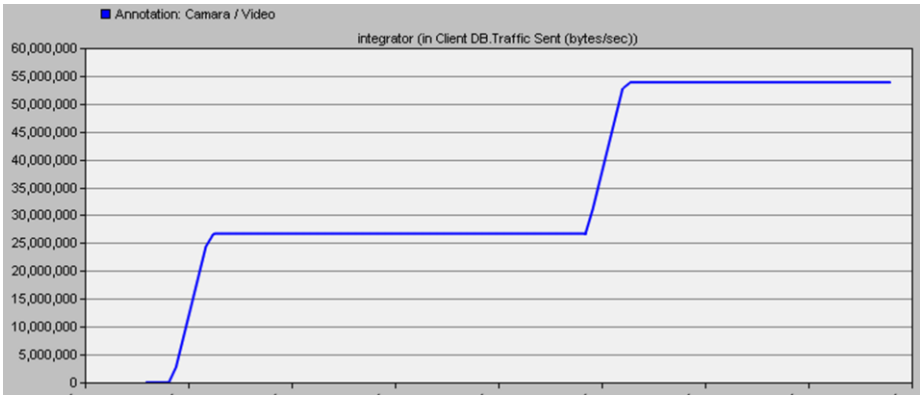


Figura A.6: Gráfico integrador del tráfico total de video enviado por una cámara.

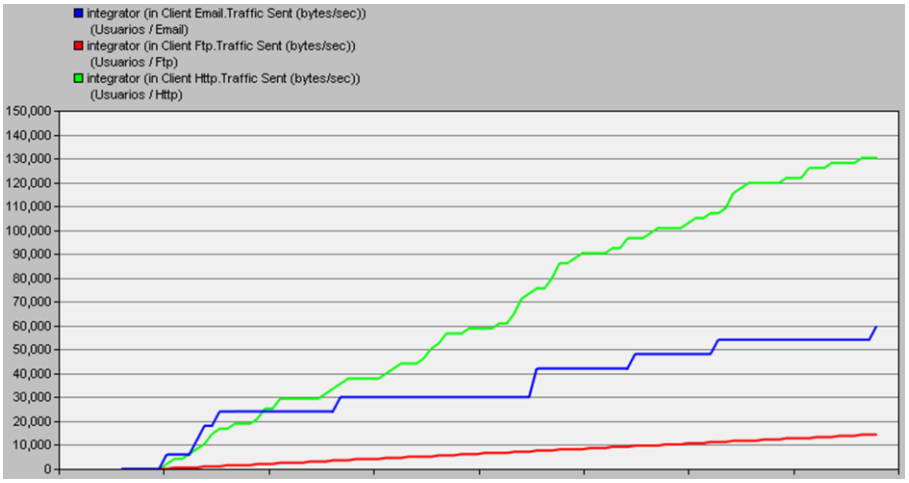


Figura A.6: Gráfico integrador del tráfico total enviado de las aplicaciones Http, Email y FTP por un usuario.

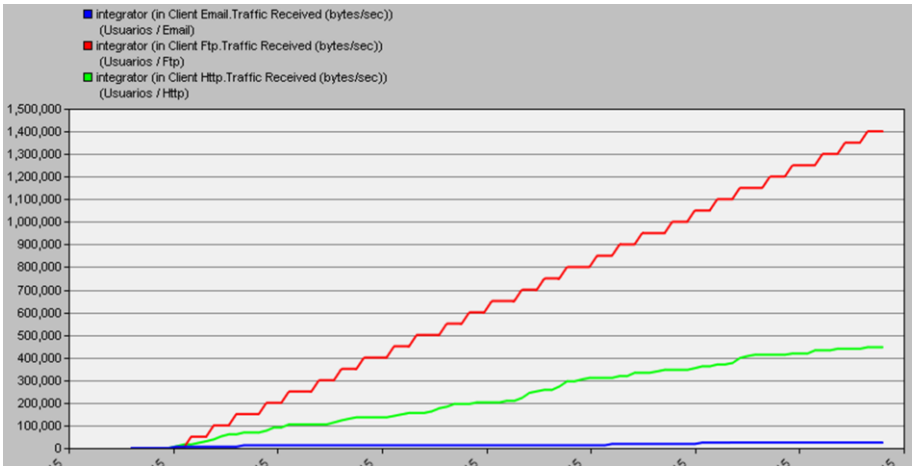


Figura A.6: Gráfico integrador del tráfico total recibido de las aplicaciones Http, Email y FTP por un usuario.