TESIS DEFENDIDA POR

Edna Dalila Pinedo Frausto

Y APROBADA POR EL SIGUIENTE COMITÉ

Dr. José Antonio García Macías
Director del Comité

Dr. Roberto Conte Galván
Miembro del Comité

Dr. Jesús Favela Vara
Miembro del Comité

Dr. Romeo Christian Velarde Montecinos
Miembro del Comité

Dr. Pedro Gilberto López Mariscal
Coordinador del programa de posgrado en Ciencias de la Computación

Dr. David Hilario Covarrubias Rosales
Encargado del Despacho de la Dirección de Estudios de Posgrado

14 de *Febrero* de 2008

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA

PROGRAMA DE POSGRADO EN CIENCIAS
EN CIENCIAS DE LA COMPUTACIÓN

ANÁLISIS DE LA APLICACIÓN DE REDES ZIGBEE EN ENTORNOS INDUSTRIALES DE MONITOREO Y CONTROL

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de
MAESTRO EN CIENCIAS

Presenta:

EDNA DALILA PINEDO FRAUSTO

Ensenada, Baja California, México, Febrero del 2008.

RESUMEN de la tesis de **Edna Dalila Pinedo Frausto**, presentada como requisito parcial para la obtención del grado de MAESTRO EN CIENCIAS en Ciencias de la Computación. Ensenada, Baja California, México. Febrero 2008.

ANÁLISIS DE LA APLICACIÓN DE REDES ZIGBEE EN ENTORNOS INDUSTRIALES DE MONITOREO Y CONTROL.

Resumen aprobado por:

Dr. José Antonio García Macías

Director de Tesis

Debido a las características de ubicuidad, movilidad y facilidad de instalación de las redes inalámbricas de sensores, se ha propuesto su uso en entornos industriales de monitoreo y control. Sin embargo, los estrictos requerimientos de estos entornos y la poca investigación realizada sobre las capacidades prácticas de las redes inalámbricas de sensores, generan dudas sobre el alcance de las aplicaciones que éstas pueden tener. La organización ZigBee Alliance ha desarrollado un conjunto de protocolos, cuyos requisitos de diseño incluyen un bajo consumo de potencia, bajo costos de instalación y mecanismos de seguridad para redes inalámbricas de sensores, teniendo como objetivo su aplicación en diferentes entornos, entre ellos el industrial. No obstante, el enfoque inicial de Zigbee Alliance ha sido la atención de los mercados de consumo final y no los industriales.

Con la finalidad de determinar el tipo de aplicaciones de monitoreo y control en que puede ser utilizado actualmente el protocolo ZigBee, se ha buscado establecer las necesidades específicas de los diferentes niveles de aplicaciones industriales. Para lograr esto, se realizó un estudio de los principales tipos de protocolos para interconexión de redes de sensores cableadas, que se utilizan actualmente en este tipo de entornos. Además se generó un banco de pruebas para verificar en qué medida el protocolo ZigBee puede cubrir estas necesidades, y se profundizó en las ventajas y desventajas específicas de ZigBee, así como las restricciones y características específicas de las aplicaciones en que puede ser utilizado. Por consecuencia, el presente trabajo pone en evidencia el alcance actual de ZigBee en cuanto a su aplicación en entornos industriales, pero también permite dilucidar sus limitaciones con la intención de atenderlas en especificaciones futuras.

Palabras clave: ZigBee Alliance, ZigBee.

ABSTRACT of the thesis presented by **Edna Dalila Pinedo Frausto** as a partial requirement to obtain the Master of Science degree in COMPUTER SCIENCE. Ensenada, Baja California, Mexico. February 2008.

ANALYSIS OF THE APPLICATION OF ZIGBEE TO INDUSTRIAL CONTROL AND MONITORING ENVIRONMENTS.

Abstract approved by:

Dr. José Antonio García Macías

Thesis Director

Due to the mobility, *easy-to-install*, and ubiquitous characteristics of wireless sensor networks, it has been proposed to use them in control and monitoring of industrial environments. However, the strict requirements of these environments and the lack of research over the practical performance of wireless sensor networks, generate doubts about the kind of applications for which they can be used. The ZigBee Alliance developed a set of protocols, with requirements which include low power consumption, low installation costs and security mechanisms for wireless sensor networks, having the industrial environment as one of its many target applications. Nevertheless, the initial approach of ZigBee has been the consumer electronics and not the industrial market.

With the aim of determining the kind of monitoring and control applications in which the ZigBee protocol can actually be used, the specific needs of the different industrial application levels have been established. To accomplish this, research over the main kinds of protocols currently used to interconnect wired sensor networks in these environments, has been done. Besides generating a test bench to verify how ZigBee can cover those needs, the specific pros and cons of this protocol have been enumerated, such as the restrictions and characteristics of the applications in which it can be used. Therefore this research work shows the actual scope of ZigBee in its application to industrial environments, but also illuminates its limitations to address them in future specifications.

Palabras clave: ZigBee Alliance, ZigBee, redes inalámbricas de sensores.
Key words: ZigBee Alliance, ZigBee, wireless sensor networks.

Dedicatoria

A mi madre, porque todo lo que soy y lo que hago tuvo comienzo en ella.

Agradecimientos

A mi madre, por todo su amor y apoyo a lo largo de mi vida.

A mi hermano, por ser mi mejor amigo y por alegrarme la vida con su compañía.

A mi padre, por su apoyo en esta etapa de mi vida.

A Adrián, porque su compañía hizo de Ensenada un hogar para mi, y por su cariño y ayuda para llevar a cabo mi objetivo.

A mi familia, por hacerme sentir como si no me hubiera ido.

A mi director de tesis José Antonio García Macías, por su ayuda, consejos y paciencia.

A los miembros del comité, Dr. C. Romeo Velarde Montecinos, Dr. Roberto Conte Galván y Dr. Jesús Favela Vara por sus consejos y ayuda en la revisión de la tesis.

A mis queridas amigas Argelia Ronquillo Méndez y Dairazalia Sánchez Cortés, por su amistad, y ayuda para la creación del congreso HIC.

A mis queridos amigos Carlos Fernando Caloca de la Parra e Isaac Noé García Garza, por su cariño y apoyo.

A mi querido amigo Christian Paúl García Martínez, por su atención a mis ratos filosóficos y por su ayuda para hacerme de las herramientas necesarias para lograr mi objetivo

A mi mejor amiga Lilia Lizeth Tello Ríos, porque aunque siempre estuvo lejos, nunca dejó de estar conmigo.

A CICESE por darme la oportunidad de lograr una de mis metas más importantes.

A Ubilogix dónde no sólo encontré apoyo en aspectos materiales sino también en el conocimiento y ánimo de sus integrantes.

A Tim Gillman y Drew Gislason por darme por su amistad y ayuda para lograr mi objetivo.

Tabla de Contenido

Página

Tabla de Contenido (Cont.

Página

Tabla de Contenido (Cont.)

Página

Lista de Figuras

Página

Lista de Figuras (Cont.)

Página

Lista de Figuras (Cont.)

Página

Lista de Tablas

Página

CAPÍTULO I

INTRODUCCIÓN

Consideradas hace 5 años como una de las tecnologías emergentes que cambiarán al mundo (Rush, 2003), las redes inalámbricas de sensores han continuado su desarrollo enfrentando requerimientos estrictos en el manejo de memoria y energía, para el diseño de aplicaciones, al mismo tiempo que ofrecen una nueva dimensión tecnológica que promete la satisfacción de un nuevo ámbito de necesidades en los sistemas inalámbricos.

Sin embargo, la investigación sobre estas redes no ha terminado, pues existen aún demasiadas preguntas que contestar sobre su funcionamiento y capacidades para aplicaciones en la vida diaria. Además, estas redes presentan grandes retos en el desarrollo de aplicaciones, debido a los limitados de recursos de memoria y energía con que cuentan los dispositivos utilizados, y a las consideraciones de robustez y confiabilidad que inherentes de las redes inalámbricas de datos.

Por estas razones tanto en la academia como en la industria se han llevado a cabo diferentes investigaciones que dirigen el desarrollo de estas redes en busca de un punto de estabilidad y confiabilidad que las hagan lo suficientemente

robustas para aplicaciones reales. Por lo anterior es necesario verificar ahora hasta qué punto este esfuerzo ha logrado sus objetivos.

I.1 Planteamiento del problema

A pesar de todo el apoyo que las redes de sensores han tenido por parte de la industria y la academia, aún hace falta mucho trabajo para lograr que las redes inalámbricas de sensores sean lo que realmente se espera de ellas. Uno de los principales objetivos de la investigación en esta área es lograr un estándar suficientemente robusto y confiable para que las aplicaciones de monitoreo y control sean factibles en ámbitos como el hogar, la industria o la medicina. Sin embargo esto no puede ser posible sin un estudio que avale las verdaderas capacidades de estas redes. Es necesario probar hasta qué punto este tipo de redes son verdaderamente confiables y robustas para ofrecer el soporte que necesitarán las aplicaciones que se desarrollarán sobre ellas.

Este problema es aún más importante en el caso de aplicaciones de monitoreo y control de procesos industriales. Debido a la falta de investigaciones que demuestren las capacidades de las redes inalámbricas de sensores, existe aún una gran desconfianza por parte de la industria en cuanto al uso de este tipo de redes para monitoreo y control de tareas críticas. En resumen, sin un estudio que avale el desempeño de las redes inalámbricas de sensores en aplicaciones

representativas de las principales necesidades de la industria, el avance en su desarrollo se dará en forma lenta y sin una apropiada dirección.

I.2 Objetivos de la investigación

Existen muchos tipos de redes inalámbricas de sensores y el llevar a cabo una verificación de todas ellas sería una tarea muy compleja. Para restringir este estudio a un protocolo en específico se realizó un estudio de las soluciones para redes inalámbricas existentes al momento de la investigación. A partir de ésta investigación se determinó que el protocolo ZigBee además de contar con el soporte más amplio por parte de la industria, es una solución utilizada y desarrollada desde hace varios años. Por todas estas razones, el trabajo de investigación aquí propuesto se restringe a un estudio sobre la especificación ZigBee, que además se encuentra disponible para la realización de las pruebas necesarias.

I.2.1 Objetivo general

El objetivo principal de este trabajo de investigación es determinar la aplicabilidad de ZigBee a los sistemas industriales de automatización y control, de manera que más allá de comprobar suposiciones acerca de su desempeño en

aplicaciones industriales, se podrá establecer el nivel de robustez y confiabilidad que puede ofrecer y el tipo de aplicaciones industriales en que podrá ser utilizado.

I.2.2 Objetivos específicos

- Identificar las características necesarias en las redes inalámbricas de sensores para aplicaciones en entornos industriales.
- Determinar las capacidades de las redes cableadas en ámbitos industriales, para verificar el grado en que son cubiertas con las características del estándar ZigBee.
- Generar un banco de pruebas para verificar las características favorables en una red ZigBee para su adaptación a entornos industriales.
- A través del análisis de resultados de las pruebas determinar las ventajas y desventajas del protocolo ZigBee en el contexto de aplicaciones industriales.
- Derivar el conjunto de aplicaciones de monitoreo y control en ambientes industriales en los que ZigBee puede ser utilizado.

I.3 Contribución al conocimiento

La contribución principal de esta investigación es la determinación de las características de las redes inalámbricas de sensores que son deseables y necesarias para su implementación en aplicaciones industriales de monitoreo y

control, tomando como ejemplo el protocolo ZigBee, uno de los estándares más apoyados por la industria.

Determinar el tipo de características que estas redes tienen actualmente, y los puntos débiles en que se debe trabajar para continuar su desarrollo en aplicaciones fuera de la academia, permitirá tener una mejor perspectiva de los verdaderos problemas a los que se enfrentan y de esta manera se puede enfocar la investigación tanto en la academia como en la industria para hacer énfasis en esos puntos débiles.

Existen casos de estudio como el que se presenta en (Poor et al, 2002) sobre el funcionamiento de redes inalámbricas de sensores en una aplicación industrial. Sin embargo, estos casos de estudio se refieren a una aplicación específica, por lo que no es posible generalizar esos resultados a otros tipos de aplicaciones. En cambio, este trabajo de investigación busca establecer un punto de referencia para el uso o no de las redes inalámbricas de sensores en aplicaciones industriales, y también determinar las áreas críticas de investigación para su desarrollo

I.4 Metodología

Para realizar esta investigación se utilizará una metodología de modelo incremental y flexible, en la que los resultados de las primeras fases permitirán la definición de las etapas subsecuentes. Sin embargo el análisis de resultados deberá

basarse en características completamente comprobables sobre el protocolo, las cuales serán determinadas en la primera etapa de investigación.

Etapas del trabajo de investigación:

- Se realiza en primer término un estudio de las aplicaciones industriales de monitoreo y control existentes. Para poder realizar este estudio, es necesario remitirse al estado del arte sobre el tema, y a la literatura correspondiente. Además se buscó el apoyo e información proveniente de asociaciones para estandarización de sistemas industriales, tales como ISA (The Instrumentation, Systems, and Automation Society). Los resultados de éste estudio se presentan en el Capítulo II.
- Se debe conocer cuáles son los sistemas utilizados en estas aplicaciones y las características que los hicieron aptos para dar soporte a las mismas. Esta información tiene las mismas fuentes que el punto anterior, pero además depende de un análisis en conjunto tanto de la importancia de ciertas características como de la capacidad para diseñar las pruebas apropiadas para su estudio. En el Capítulo II se describen brevemente las características principales de éstos sistemas.
- A partir de este estudio se determinan cuáles son las características deseables en las redes inalámbricas de sensores para aplicaciones de este tipo, las cuales se presentan en el Capítulo II.

- Se determinan las características principales del protocolo ZigBee, con un enfoque dirigido a las aplicaciones en entornos industriales de monitoreo y control. Este estudio se muestra en el Capítulo III.
- Se realiza el diseño de las pruebas apropiadas con base en estas características definidas en el Capítulo II para determinar hasta qué grado un estándar como ZigBee cumple con ellas. Para esto, se establece un banco de pruebas que permita observar en forma independiente el desempeño del estándar ZigBee con respecto a cada una. Estas pruebas se describen en el Capítulo IV.
- Los resultados de las pruebas, mostrados en el Capítulo V, determinan el tipo de aplicaciones en las que este estándar puede ser utilizado. Es decir, una vez que se conozcan las características de las aplicaciones a las cuales ZigBee puede dar el soporte apropiado, se analiza su desempeño y la posibilidad de utilizarlo en determinados tipos de aplicaciones industriales. Para lograr esto es necesario revisar el estudio realizado en el Capítulo II sobre los tipos de aplicaciones existentes. Las conclusiones de ésta comparación entre las soluciones existentes y los resultados obtenidos sobre el desempeño del protocolo ZigBee, se muestran en el Capítulo VI.

CAPÍTULO II

REDES INDUSTRIALES DE MONITOREO Y CONTROL

II.1 Introducción

Existe una gran variedad de aplicaciones para las redes de sensores dentro de los entornos industriales, definidos como aquellos ambientes físicos, creados para albergar y permitir los procesos y actividades que forman parte de la creación de productos o servicios, a partir de la transformación o tratamiento de materias primas. Algunos ejemplos de aplicaciones en entornos industriales son la automatización de edificios, control de redes de servicios (agua, electricidad, etc.), comunicación y control en sistemas empotrados, monitoreo y control de aplicaciones de manufactura y procesos industriales, etc., cada uno de estos tipos de aplicaciones cuenta con características y requerimientos completamente diferentes. Debido a esto, el diseño de un sistema estándar para interconexión de sensores, actuadores y dispositivos o sistemas de control ha resultado un proceso tardío y complejo. A principios de los 80s comenzaron los proyectos para desarrollar un protocolo de comunicación que satisficiera las necesidades de la amplia gama de aplicaciones existentes en ese momento, disminuyendo los costos y complicaciones de instalación (Felser y Sauter, 2002).

Las características tan diferentes de las aplicaciones a las que estaba dirigida esta estandarización, aunadas a la gran variedad de soluciones propietarias existentes, dificultaron la creación de un protocolo sencillo, y promovieron la generación de unos cuantos estándares compuestos por una gran variedad de protocolos con pequeñas diferencias entre ellos.

Uno de los proyectos más importantes desarrollados durante este periodo fue *Fieldbus* en sus diferentes variantes o perfiles, desarrollado por el gobierno de Estados Unidos en conjunto con varios países de Europa como Francia y Alemania, con la finalidad de crear un estándar que permitiera la compatibilidad con los principales sistemas de la época. Debido a la fuerte competencia entre los sistemas y organizaciones existentes por conseguir la estandarización, *Fieldbus* es hoy un diseño general o guía para la implementación de siete diferentes tipos de sistemas.

Por otro lado el proyecto CAN (Controller Area Network), desarrollado por la compañía Bosch específicamente para la manufactura de carros en Alemania (Corrigan, 2002), es actualmente otro de los protocolos más importantes en el área de redes industriales de control, principalmente para sistemas empotrados y con requerimientos de respuesta en tiempo real. Además de OpenCAN, una de las versiones que utilizan al protocolo CAN, la organización europea CENELEC (Comité Européen de Normalisation Electrotechnique) define el protocolo AS-i como un estándar *Fieldbus* necesario para satisfacer las necesidades europeas de

estandarización que el IEC (International Electrotechnical Commission) deja atrás (Thomesse, 2005).

Además del estándar *Fieldbus*, se ha buscado la integración de redes de datos con redes de monitoreo y control en los estudios sobre Industrial Ethernet, con la finalidad de mejorar características como ancho de banda o número máximo de dispositivos manteniendo las capacidades de respuesta en tiempo real. Debido a este tipo de investigación se han generado nuevos protocolos y nichos de aplicación para redes como estas.

En la actualidad las redes cableadas de sensores siguen siendo las más importantes en aplicaciones industriales. Existen muchas soluciones más para resolver los problemas de las comunicaciones industriales. Sin embargo, debido al apoyo por parte de la industria con el que cuentan las tecnologías mencionadas en éste capítulo, y su natural adopción en la mayoría de los entornos industriales de monitoreo y control, podemos considerar que un estudio profundo de las características de estas tecnologías en específico, nos permitirá un entendimiento más completo de las necesidades del tipo de aplicaciones a las que este tipo de soluciones están dirigidas.

La finalidad principal de este capítulo es mostrar las características comunes más importantes de los tipos de redes de sensores que se utilizan en la industria actualmente. Para esto primero se explica el modelo jerárquico de aplicaciones de acuerdo al cual se clasifican los sistemas existentes para dar solución a

determinados tipos de aplicaciones. A continuación se definen las principales características que serán tomadas en cuenta para el análisis y comparación de estos sistemas y finalmente se nombran y explican los sistemas más representativos.

II.2 Modelo jerárquico de aplicaciones.

Para facilitar el diseño de soluciones para intercomunicación de dispositivos, el NBS (National Bureau of Standards) en los Estados Unidos, definió una arquitectura de modelo jerárquico que dio a conocer en 1987. Este modelo permite distinguir las características de los diferentes niveles de aplicación de las soluciones y así diseñar protocolos más apropiados para cada uno. En la Tabla Ise muestra este modelo (Thomesse, 2005).

Figura 1. Arquitectura Jerárquica (NBS)

Las diferentes tecnologías creadas para entornos industriales pueden clasificarse de acuerdo a esta jerarquía, dependiendo del tipo de dispositivos que comuniquen. Como puede observarse el nivel más bajo de la jerarquía es el encargado de conectar los sensores y actuadores a sus respectivos controladores. El siguiente nivel comprende la comunicación para el control de máquinas, ya sea para el intercambio de datos o simplemente la transmisión de comandos. De igual manera en el tercer nivel la comunicación se refiere al intercambio de datos entre las celdas o células de control que pueden contener la información de varias máquinas o secciones de una fábrica. Finalmente se tiene el nivel de mayor abstracción para el área de control, el de la fábrica que puede contener como su

nombre lo dice la interconexión necesaria para la transmisión de datos entre varias secciones de la fábrica. Y por último, se tiene la jerarquía de empresa para aquellos dispositivos que más que servir como puntos de monitoreo o control intercambiaran información necesaria para la empresa y referente a las fábricas que incluya, ya sea información de tipo administrativo o comunicación entre diferentes secciones de la empresa.

Otra forma de clasificación de las aplicaciones industriales depende del tipo de información que pasa por la red. De esta manera podemos tener aplicaciones de monitoreo, en las que la información transmitida a través de la red consiste únicamente en los datos medidos por los dispositivos, por lo que la comunicación se da en un solo sentido, del dispositivo terminal hacia el dispositivo recolector de los datos. A las aplicaciones en que, dependiendo del valor de los datos enviados al recolector, se toma una decisión y se transmiten comandos hacia los dispositivos actuadores, se les llama aplicaciones de control; la comunicación en los dos sentidos es una de las características principales de este tipo de aplicaciones. Por último las redes para transmisión de datos se refieren al envío de información que no necesariamente se refiere a estados de variables ni comandos a ejecutar, sino más bien se transmite información corporativa por lo que un mayor ancho de banda es necesario y las restricciones de tiempo de respuesta pueden ser más relajadas. La distinción de los diferentes niveles jerárquicos de acuerdo a ésta clasificación se muestra también en la Figura 2.

La finalidad de esta investigación es definir el ámbito de aplicaciones en el que puede ser ubicado un protocolo para redes inalámbricas de sensores como ZigBee dentro del modelo jerárquico mostrado. Para poder definir la posición de ZigBee dentro de este modelo, es necesario saber las características de los diferentes niveles, por lo cual, en las siguientes secciones se analizan las características principales de las redes cableadas más utilizadas actualmente en éstos ámbitos. Una vez definidas las características se compararán con las de ZigBee para verificar la posibilidad de posicionarlo en algún nivel dentro del modelo, o bien detallar los cambios en la arquitectura del protocolo que son necesarios para su uso en ámbitos industriales.

II.3 Características principales de las redes de sensores.

Para poder analizar las redes de sensores es necesario revisar algunas de sus características comunes más importantes, facilitando de esta manera su comparación y clasificación. A continuación se definen las características comunes más importantes de las redes de sensores (Sareen, 2003).

- **Jerarquía**. Este término se refiere al nivel, dentro del modelo de la Figura 1, en que se encuentra la red utilizada dependiendo del tipo de dispositivos que se conectarán a través de ella.

- **Ancho de banda.** Cantidad de información que puede ser transmitida en un tiempo fijo determinado.
- **Distancia.** Se refiere a la distancia máxima de separación entre dos dispositivos para que el envío de mensajes esté asegurado.
- **Número de dispositivos.** Cantidad máxima de dispositivos que pueden conectarse y comunicarse entre sí dentro de una red.
- **Tamaño de mensajes.** Cantidad máxima de bytes de carga útil que pueden ser enviados en un mismo mensaje.
- **Consumo de potencia.** Debido a que los dispositivos inalámbricos preferentemente deben depender de una batería como fuente de energía, su consumo en estos dispositivos debe ser verificado.
- **Respuesta en tiempo y variación.** Cantidad de tiempo transcurrido entre el final de una petición de un dispositivo de cómputo y el comienzo de la respuesta.
- **Integridad de datos.** Se refiere al porcentaje esperado de errores en la información transmitida.
- **Seguridad.** Para este estudio en específico nos referimos a la capacidad de la red para evitar que la información que pasa a través de ella pueda ser interceptada por personas o sistemas ajenos a la misma.
- **Eficiencia.** Este término se refiere a la cantidad de trabajo extra necesario para el envío de mensajes. Esta cantidad de trabajo esta determinada por tres factores:

- Sobrecarga: datos adicionales necesarios para el envío del mensaje (tramas de las diferentes capas del protocolo)
- Cantidad de mensajes.
- Trabajo de la unidad de procesamiento (CPU, en inglés Computer Processor Unit) que actúa como anfitrión.
- **Redundancia.** Capacidad de la red de resolver la pérdida de rutas o bien de dispositivos.
- **Capacidades de interconexión.** Las capacidades de una red de comunicación industrial se refieren a la posibilidad que tiene esta red de comunicarse con algún otro tipo de protocolo, tales como RS232, RS422, or RS485, DeviceNet, Modbus, Profibus, Ethernet, etc.
- **Método de acceso.** Se refiere a la técnica utilizada por los dispositivos para adquirir y utilizar el medio de comunicación compartido.
- **Topología.** Patrón descrito por la interconexiones entre los dispositivos.
- **Soporte.** Aunque difícilmente cuantificable, es importante tomar en cuenta las posibilidades de apoyo por parte de los expertos para la solución de problemas, así como el mantenimiento de compatibilidad con las nuevas tecnologías o bien la mejora continua del mismo protocolo.

Con base en las características anteriormente definidas, en la siguiente sección se realiza el análisis de cuatro importantes redes industriales utilizadas actualmente. Este análisis permitirá encontrar parámetros de comparación con éste tipo de redes dependiendo del tipo de aplicaciones en el que son utilizadas, para posteriormente verificar los valores de éstos parámetros con los de una red inalámbrica como ZigBee para posicionarlo en el modelo jerárquico mostrado en la Figura 1.

II.4 Redes industriales de sensores utilizadas en la actualidad

Para una mejor comprensión de las características de las redes cableadas utilizadas en ambientes industriales, es necesario hacer una revisión de aquellas redes que pueden considerarse como las más importantes o las más utilizadas. Este capítulo realiza una revisión de éstas redes y sus características más importantes.

II.4.1 Fieldbus

Definido como red para interconexión de dispositivos de campo tales como sensores, actuadores, controladores de campo como PLCs, reguladores, controladores de dirección, etc., e interfaces hombre-máquina (Thomesse, 2005). El estándar fieldbus es el resultado del esfuerzo por parte del IEC para el desarrollo de un protocolo común que permita la interconexión de dispositivos de campo. Sin

embargo, antes de la definición de fieldbus como un estándar existían una gran cantidad de sistemas diferentes. Esta situación derivó en la creación de una especificación poco precisa conformada por 7 perfiles de aplicación diferentes que además pueden ser subdivididos. En la Tabla I (Thomesse, 2005) se muestran estos CPFs (Communication Profile Families) con sus implementaciones más representativas y algunas características que los distinguen, según su definición en el estándar IEC 61158 publicado en el 2000 y la definición de perfiles del estándar IEC61784.

Además de los estándares *Fieldbus* IEC 61158 e IEC 61748 el grupo CENELEC publica actualizaciones de 4 especificaciones para proveer un modelo internacional que complete al estándar de IEC. Estas cuatro actualizaciones fueron EN50170 referente a P-Net, Profibus y WorldFIP, EN50254 para mejorar el desempeño de INTERBUS, PROFIBUS DP y Device WorldFIP, EN50325 que cubre los derivados del protocolo CAN como DeviceNet, SDS y CANOpen y EN50259 que define el protocolo de actuadores e interfaces AS-i.

Tabla I. CPF (Communication Profile Families) de fieldbus

Perfil	Nombre	Características Especiales	Método de Acceso	Nodos Máx.
CPF-1/1	FF (H1)	Bloques funcionales para control descentralizado	Productor-consumidor con distribuidor	32
CPF-1/2	FF (HSE)		CSMA/CD	30
CPF-1/3	FF (H2)		Productor-consumidor con distribuidor	32
CPF-2/1	ControlNet	Optimizado para aplicaciones de fábrica	Productor-consumidor	99
CPF-2/2	EtherNet/IP			30
CPF-3/1	PROFIBUS-DP	Optimizado para E/S remotas	Maestro-esclavo con token-passing	126
CPF-3/2	PROFIBUS-PA	Optimizado para control de procesos		32
CPF-3/3	PROFInet	Objetos de automatización distribuidos	Productor-consumidor	30
CPF-4/1	P-Net RS-485	Capacidades Multi-net	Maestro-esclavo con token-passing	32
CPF-4/2	P-Net RS-232			
CPF-5/1	WorldFIP	Base de datos en tiempo real distribuida	Productor-consumidor con distribuidor	256
CPF-5/2				
CPF-5/3				
CPF-6/1	INTERBUS	Optimizado para E/S remotas	Mono-maestro con cambio de registro sincronizado	256
CPF-6/2	INTERBUS TCP/IP			
CPF-6/3	INTERBUS Subset			
CPF-7/1	Swiftnet transport	Optimizado para aeroplanos	Productor-consumidor con distribuidor	1024
CPF-7/2	Swiftnet full snack			

Debido a que los protocolos CAN y AS-i representan niveles diferentes del modelo jerárquico de aplicaciones, se les analiza posteriormente con mayor profundidad. De esta manera resulta más sencillo caracterizar cada nivel de aplicaciones. De igual manera EtherNet/IP se distingue en los niveles del modelo jerárquico debido a sus capacidades para aplicaciones en tiempo real con un mayor ancho de banda y número de dispositivos, por lo que se toma también como distintivo de los niveles de control y transmisión de datos.

II.4.2 Clasificación de estándares dentro del modelo jerárquico de aplicaciones.

Como ya se mencionó la colección de protocolos aceptados como estándares se reduce a siete para la IEC y se agregan un par más para la CENELEC, sin embargo la cantidad de protocolos existentes es mucho más grande y cada uno de estos protocolos fue definido para un nicho específico dentro del modelo jerárquico de aplicaciones. A continuación en la Figura 2 (Verhappen, 2002) se muestra el rango de aplicaciones para las que fueron diseñados estos protocolos.

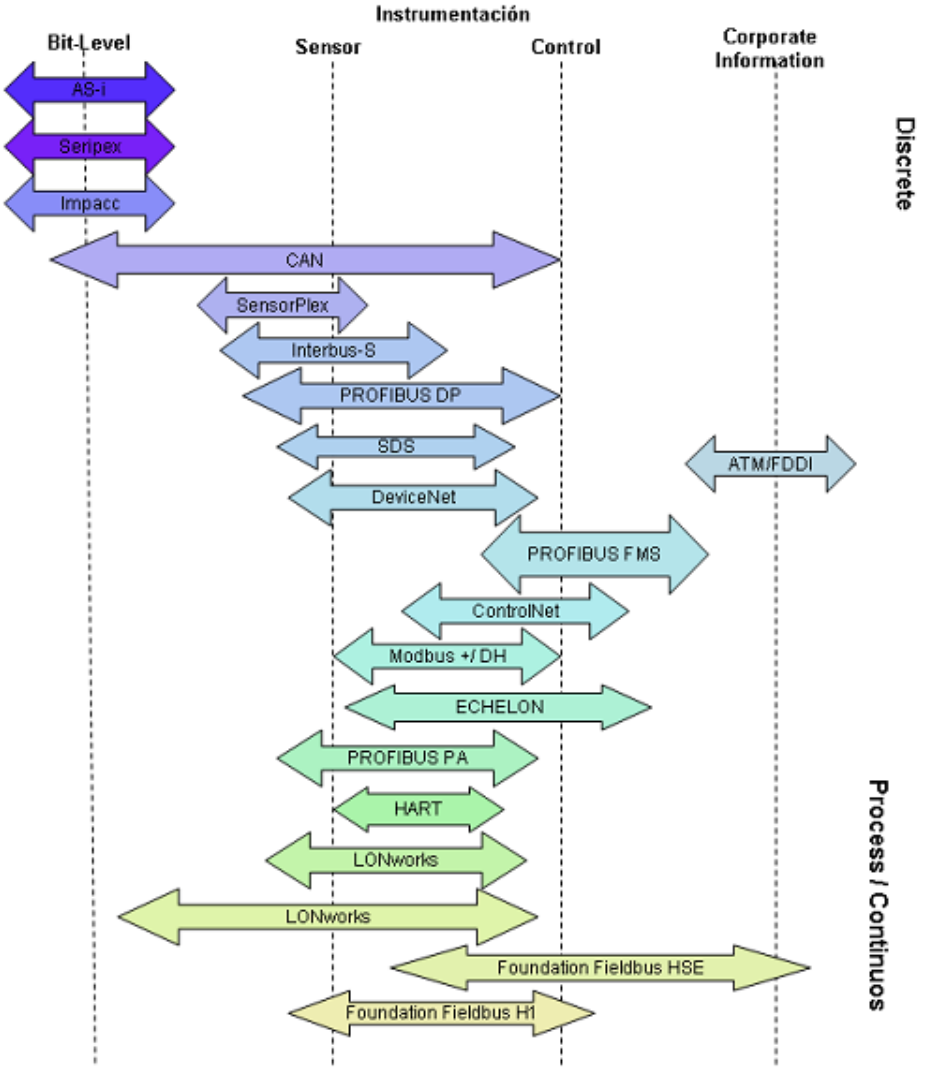


Figura 2. Clasificación de Redes Industriales de Sensores

Debido a que el análisis realizado en este trabajo de investigación se refiere específicamente a aplicaciones de monitoreo y control, se han tomado los protocolos más representativos de los niveles de aplicación mostrados en la Figura 2. Estos protocolos son, AS-i para la interconexión de sensores y actuadores binarios; CAN para la interconexión de sensores y actuadores en redes de

monitoreo y control; Foundation Fieldbus H1 y por último EtherNet/IP, como el protocolo de Industrial Ethernet más utilizado para la conexión entre el nivel de control e intercambio de información de planta, debido a su comunicación transparente con dispositivos DeviceNet.

II.4.3 Fieldbus Foundation

Foundation Fieldbus aparece en 1994 como un intento por diseñar un protocolo estándar internacional para ambientes peligrosos. Su arquitectura de comunicación basada en el modelo OSI se compone de tres elementos principales: capa física, pila de comunicación y capa de aplicación de usuario (Samson, 2007).

La capa física de Foundation fieldbus puede ser H1 o HSE, HSE sin embargo está enfocada al uso de dispositivos Ethernet para el manejo de un mayor ancho de banda, por lo que su nivel de aplicación en el modelo jerárquico se encuentra al nivel de los protocolos Industrial Ethernet. En cambio H1 permite la intercomunicación y transmisión de energía eléctrica a los dispositivos conectados con un ancho de banda menor, de manera que su nivel de aplicación se encuentra entre la interconexión de sensores y comunicación de comandos de control. Para la caracterización de los protocolos Industrial Ethernet se describirá el protocolo más utilizado EtherNet/IP, es por esto que la versión H1 de fieldbus resulta más interesante ya que define mejor el nivel de aplicaciones de monitoreo y control.

La pila de comunicaciones del Fieldbus Foundation consiste en mantener el control centralizado de la comunicación a través de LAS (Link Active Scheduler). Pero permite a todos los dispositivos la capacidad de enviar mensajes por lo que se dice que utiliza un modelo de comunicación distribuida. Únicamente los dispositivos *Link Master* tienen la capacidad de convertirse en LAS. La posibilidad de tener más de un *Link Master* permite redundancia en el sistema (Samson, 2007).

La pila de comunicaciones está compuesta de dos capas, la capa de enlace de datos y la capa de aplicación. La capa de aplicación que contiene a la FAS (Fieldbus Access Sublayer) y la FMS (Fieldbus Message Specification), es la interfaz entre la capa de aplicación del usuario y la capa de enlace de datos. La FAS se encarga de crear VCRs (Virtual Communication Relationships) utilizados por la subcapa superior FMS para ejecutar tareas. Existen varios tipos de VCRs, Publicista/Suscriptor, Cliente/Servidor o Distribución de reporte. A través de estos VCRs se transmite la entrada y salida de datos de un bloque de función el cual especifica la funcionalidad de un dispositivo. La FMS provee servicios para una comunicación estandarizada a través de la asignación de servicios de comunicación a objetos definidos. La FMS también define VFD (Virtual Field Devices) para facilitar la obtención de descripciones de los dispositivos de campo y la información que contienen desde cualquier punto de la red.

Para darle interoperabilidad al protocolo Foundation, se definen en forma uniforme las funciones de los dispositivos y las interfaces de aplicación a través de

un modelo de bloques, para la asignación de funciones de un dispositivo. Estos bloques de descripción pueden ser de tres tipos: recursos, transductores y funciones. El primer tipo describe datos generales del dispositivo como su nombre, fabricante y versiones de hardware o firmware. El bloque de transductores le da posibilidades al dispositivo para afectar con otra información los datos de entrada y salida del dispositivo. El bloque de funciones como lo indica su nombre define las funciones del dispositivo y la forma de acceder a ellas.

A continuación se muestra un compilado de las características principales del estándar Fieldbus Foundation H1, debido a que por sus cualidades es utilizado para conexión de sensores y actuadores así como para el control de máquinas. Permitiéndonos caracterizar un nivel diferente del modelo jerárquico de aplicaciones, que va desde aplicaciones de monitoreo, con la conexión simple de sensores y actuadores, hasta aplicaciones más complejas de control.

II.4.3.1 Foundation Fieldbus H1

Basado en la especificación IEC 61158, utiliza una codificación Manchester con una tasa de transferencia de 31.25kbps, permite la transmisión de energía a los dispositivos a través del bus. Tiene capacidad para topologías de línea y con el uso de cajas de unión pueden crearse topologías tipo estrella o combinaciones en árbol. Dependiendo del tipo de cable los segmentos H1 pueden tener distancias desde 200m hasta 1900m

Tabla II. Características Principales – Fieldbus Foundation H1

Características	Foundation H1
Jerarquía	Conexión de S/A
Ancho de banda	500kbps - 31.25kbps
Distancia máxima	500m @ 125kb/s 100m @ 500kb/s - 1900m
Tamaño de la red	32
Tamaño de mensaje	No especificado
Consumo de potencia	No especificado
Respuesta en tiempo y variación	5ms Manufactura 20 ms Control de procesos
Integridad de los datos	1 error cada 20 años (6.3×10^{-11})
Seguridad	No especificado
Eficiencia	Diferentes tipos de dispositivos para LAS
Redundancia	Multiple LAS, estrategia de control distribuida.
Capacidades de interconexión	HSE, AS-i
Método de acceso	Controlador de ciclo LAS
Topología	Bus, árbol
Soporte	Variedad de compañías

II.4.4 CAN (Controller Area Network)

Diseñado por la compañía Bosch en Alemania el estándar CAN o ISO 11898 es un protocolo de comunicación *broadcast* serial y multi-maestro, centrado en el envío de mensajes cortos *broadcast* para consistencia de datos en toda la red (Thomesse, 2005). Algunas de sus características son tasa de datos de 1Mbps, alta inmunidad a la interferencia, habilidad de autodiagnóstico, corrección de errores y direccionamiento basado en el contenido del mensaje.

La característica más importante de este protocolo es su método de acceso CSMA/CD (en inglés Carrier Sense Multiple Access with Collision Detection) con prioridad no destructiva debido a que evita el efecto *thrashing* existente en otras redes CSMA/CD, aunque esta técnica deriva en restricciones en la señal de la capa física y en la extensión geométrica de la red (Hasnaoui, 2001). Para el método de acceso de este protocolo existen dos tipos de bits, dominante y recesivo, donde el bit dominante sobrescribe al recesivo. La prioridad de acceso al bus está definida con el valor de los bits de identificación y cuando dos dispositivos comienzan la transmisión al mismo tiempo, los bits de identificación dominante sobrescribirán a los del recesivo. Al leer un valor diferente al transmitido, el nodo transmisor comprende que ha perdido el bus y detiene su transmisión, permitiendo al dispositivo que gana el bus simplemente continuar enviando su mensaje sin que

éste haya sido destruido o descartado. El dispositivo que pierde el bus detiene la transmisión inmediatamente e intenta volver a transmitir solo cuando el mensaje prioritario ha sido totalmente enviado. Gracias a esta característica CAN tiene la capacidad de ser utilizado en aplicaciones de control en tiempo real (Corrigan, 2002).

El estándar CAN fue definido en base al modelo OSI (Open Systems Interconnection) para la capa física y la de enlace de datos. En su primera versión fue definido con un identificador de 11 bits y un ancho de banda de 125 kbps, posteriormente se definieron las versiones 2.0A y 2.0B con un ancho de banda de 1Mbps y un identificador de 29 bits.

Existen 4 tipos de mensajes en el protocolo CAN (Corrigan, 2002):

- De datos. Es utilizado para el envío de hasta 8 bytes de información. El nodo receptor genera un bit para sobrescribir el campo ACK e indicar una transmisión completa y correcta.
- Remoto. Permite a un nodo solicitar a otro que realice una transmisión de datos, se distingue del anterior por el bit RTR.
- Error. Es generado cuando uno de los nodos encuentra un mensaje que contiene algún error, el resto de los nodos repite este mensaje de error para que al ser avisado el nodo transmisor del mensaje erróneo lo retransmita.

- Sobrecarga. Parecido al mensaje de error, es enviado por un nodo cuando se encuentra demasiado ocupado para obtener un retraso extra entre mensajes.

El alto nivel de robustez de CAN se debe a los cinco métodos de verificación de errores que realiza, tres de los cuales son a nivel del mensaje, que consisten en la verificación de los valores de los campos CRC y ACK y de los bits delimitantes de los campos SOF, EOF y ACK. Los otros dos métodos de verificación son a nivel de bit, uno de ellos consiste en que el nodo transmisor lea cada uno de los bits que trasmite, si encuentra que alguno es diferente transmite un mensaje de error y reinicia la transmisión. Por último a nivel de bit se verifica la regla de *stuffing*, la cual dicta que después de cinco bits consecutivos con el mismo valor, el siguiente debe ser complementario (Corrigan, 2002).

Entre las principales aplicaciones del protocolo CAN se encuentran: electrónica automotriz, unidades de control de motores, sensores, automatización de edificios y fábricas, sistemas de control empotrados, dispositivos médicos y aplicaciones domésticas, etc. Debido a sus características de robustez y consistencia, así como sus capacidades para aplicaciones en tiempo real, este protocolo ha sido ampliamente utilizado. En la Tabla III se muestran las características principales de este protocolo mencionadas anteriormente.

Tabla III. Características Principales - CAN

Características	Protocolo CAN
Jerarquía	Conexión de S/A
Ancho de banda	125kbps – 1Mbps
Distancia máxima	40m
Tamaño de la red	30 nodos
Tamaño de mensaje	8 bytes de datos
Consumo de potencia	Indiferente, se asume la disponibilidad de energía a través del cableado.
Respuesta en tiempo y variación	Capacidad para tiempo real
Integridad de los datos	Cuenta con 5 métodos de corrección y detección de errores.
Seguridad	No
Eficiencia	64/115= 56% para estandar 64/135= 47% para versión extendida 2.0B
Redundancia	Mensajes broadcast enviados a todos los nodos y capacidad hot-plug.
Capacidades de Interconexión	Ninguna
Método de acceso	CSMA/CD-NDA
Topología	Bus
Soporte	Bosch

II.4.5 AS-i

La finalidad principal de AS-i era la creación de una técnica que permitiera economizar el cableado para sensores y actuadores utilizando un mismo cable para transmisión de datos y de energía. Las especificaciones de esta técnica fueron diseñadas por 11 empresas relacionadas con el área en el año 1990, fue así como

nació la AS International Association[1] en 1991 como la encargada de dar impulso al diseño de aplicaciones que utilicen esta especificación. (Siemens, 1999).

La solución más importante que utiliza esta especificación es AS-Interface un diseño de la compañía SIEMENS, que cumple todos los requisitos de la técnica AS-i. Debido al soporte ofrecido por esta compañía, AS-Interface es casi indistinguible de AS-i.

Esta técnica funciona con un muestreo cíclico bajo el paradigma maestro-esclavo. El sistema es mono-maestro, una vez conectados los esclavos al maestro, éste realiza un muestreo ordenado para envío y requisición de datos. Debido a que el tamaño de mensajes siempre es el mismo, puede asegurarse un tiempo máximo de muestreo de 5ms para dispositivos estándar. Además de los dispositivos AS-i maestros y esclavos estándar con un espacio de direcciones de 4 bits que permite la conexión de hasta 31 esclavos a cada maestro, existen los dispositivos con espacio de direcciones extendido. El maestro AS-i extendido soporta un total de 31 direcciones ya sea para la conexión de 31 esclavos AS-i estándar o 62 esclavos AS-i extendidos. Para lograr esto los esclavos AS-i extendidos utilizan una de las salidas binarias como identificador A o B, duplicando el espacio de direcciones. Únicamente los esclavos tipo A pueden ser operados por un maestro AS-i estándar debido a que estos son lo que utilizan la salida binaria para distinguir entre A y B,

[1] AS-Interface http://www.as-interface.net

la conexión de un esclavo tipo B solo provocaría un error en la red, por lo que el maestro lo deshabilitaría (Kriesel, 1999).

Los esclavos AS-i estándar tienen cuatro bits de entrada y cuatro de salida, de modo que en una red estándar completa se tendría un total de 124 entradas y 124 salidas binarias. En cambio los esclavos AS-i tipo A con espacio de direcciones extendidas utilizan uno de sus bits de salida para identificación, lo cual les deja un total de 3 bits de salida y 4 bits de entrada. En el caso de los esclavos tipo B, conservan sus 4 bits de entrada y de salida, lo anterior permite que una red completamente formada por dispositivos con espacio de dirección extendida tenga un total de 248 entradas y 186 salidas.

Otra consecuencia importante debida al uso de esclavos extendidos es el aumento en el tiempo de muestreo. Debido a que la única diferencia en la dirección para los esclavos es el bit de tipo A o B, solo puede muestrearse uno en cada ciclo, por lo que el tiempo de muestreo para esclavos de este tipo se duplica. Aún así puede asegurarse que para el caso de una red completa con dispositivos extendidos el tiempo máximo de muestreo será de 10ms para cada dispositivo.

Existe un aumento en el costo de los dispositivos de dirección extendida, debido a la necesidad de duplicar la imagen de memoria en el maestro y configurar el host para el direccionamiento apropiado, sin embargo existe también una reducción de costo por el incremento en la usabilidad del maestro para una mayor cantidad de esclavos.

Debido a que este protocolo fue optimizado para la conexión de sensores y actuadores, presenta una gran cantidad de ventajas en este nivel, puede operar en condiciones ambientales difíciles, es confiable y seguro, tiene capacidades para aplicaciones en tiempo real, de fácil instalación y comunicación con niveles más altos. A continuación la Tabla IV muestra las características principales de este tipo de red.

Tabla IV. Características Principales - ASi

Características	**AS-i**
Jerarquía	Conexión de S/A
Ancho de banda	49.6kbps
Distancia máxima	100m
Tamaño de la red	31 – 62
Tamaño de mensaje	4 entradas y 4 salidas binarias estándar y extendido tipo B 4 entradas y 3 salidas extendido tipo A
Consumo de potencia	No especificado
Respuesta en tiempo y variación	5-10 ms por ciclo dependiendo del espacio de direcciones
Integridad de los datos	No
Seguridad	No
Eficiencia	100%
Redundancia	No
Capacidades de interconexión	IEthernet

Método de acceso	Muestreo cíclico maestro-esclavo
Topología	Arbol
Soporte	Simatec – siemens AS International Association

II.4.6 Industrial Ethernet

Debido a su facilidad de uso e instalación, bajo precio y características de desempeño Ethernet se ha convertido en la red de área local más importante. Por esta razón se han dirigido esfuerzos para su introducción en ambientes de control y monitoreo industrial, sin embargo, su naturaleza no determinística le ha privado de ser útil en áreas importantes del ámbito industrial debido a su poca capacidad para manejo de tráfico en tiempo real.

Aún así los esfuerzos por darle a Ethernet cabida en éstas áreas han llevado al desarrollo de soluciones que le permitan un desempeño apropiado en aplicaciones de tiempo real, sin importar lo diferentes que sean. A este conjunto de soluciones se les llama Industrial Ethernet.

Las modificaciones para darle capacidades de tiempo real a Ethernet se han hecho en diferentes niveles (Felser, 2005), algunas integran los cambios por encima de los protocolos TCP/IP, permitiendo una comunicación transparente más allá de la red de control y teniendo incluso la posibilidad de una conexión a Internet. Otras modificaciones pueden cambiar el protocolo TCP/IP e incluso Ethernet mismo,

aunque por supuesto disminuye la capacidad de comunicación, fuera de los límites de la red de control.

La revista Control Engineering[2] realizó una encuesta entre sus suscriptores, sobre el uso y planes para Ethernet e IEthernet. En esta encuesta se denota la preferencia de los suscriptores hacia el uso o plan de uso del protocolo EtherNet/IP.

EtherNet/IP apareció en el 2001, tiene como base el protocolo CIP (Common Industrial Protocol) que define un marco de trabajo para la implementación de Ethernet/IP con una arquitectura de 7 capas, similar al modelo OSI. El protocolo CIP es implementado por encima de la capa de transporte, lo que permite una completa transparencia al comunicarse con otras redes Ethernet. En la Figura 3 se muestra la arquitectura del protocolo Ethernet donde se observa la adaptación del CIP a Ethernet (ODVA, 2007), y en la Tabla V se muestran las características más importantes de una red EtherNet/IP.

[2] Control Engineering - http://www.controleng.com/article/CA6396565.html

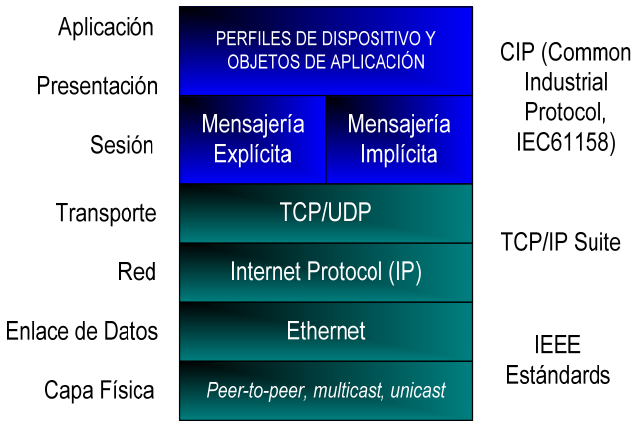


Figura 3. Arquitectura Ethernet/IP

Tabla V. Características Principales - Industrial Ethernet

Características	Ethernet/IP
Jerarquía	Control de maquinaria
Ancho de banda	10/100/1000 Mbit/s
Distancia máxima	100m – 120km dependiendo el tipo de cable
Tamaño de la red	Ilimitado
Tamaño de mensaje	1500 bytes
Consumo de potencia	No especificado
Respuesta en tiempo y variación	Interruptores,trafico priorization, modelo productor -consumidor
Integridad de los datos	Checksum VLAN
Seguridad	Firewall
Eficiencia	No determinado

Redundancia	IEEE Standar (Spanning Tree, Link aggregation), Anillo, Dual Homming
Capacidades de interconexión	DeviceNet
Método de acceso	CSMA/CD
Topología	Línea, árbol, estrella o anillo
Soporte	ODVA, vendors

Ahora que se han caracterizado estas redes es posible recabar una serie de requerimientos respecto a las características más importantes de una red, para determinar la jerarquía de aplicaciones en que puede ser utilizada. En este trabajo de investigación se busca encontrar el área de aplicación de una red inalámbrica de sensores, sin embargo, debido a la debilidad intrínseca del medio de transmisión de las redes inalámbricas, algunas de las características de las redes de sensores cableadas pueden ser demasiado estrictas para las redes inalámbricas que existen hoy. Por esta razón los grupos de investigación en esta área han definido de otra manera los tipos de aplicaciones industriales en los que las redes inalámbricas de sensores pueden ser utilizados, en la siguiente sección se describe con más detalle esta definición.

II.5 Estandarización en automatización

Para facilitar el estudio y desarrollo de un protocolo estándar para uso industrial, existen varias organizaciones que trabajan en la investigación de las

mejores opciones para su implementación. Una de las organizaciones más importantes que actualmente busca propuestas para el diseño de un protocolo para redes inalámbricas industriales es ISA (The Instrumentation, Systems and Automation Society). Fundada en 1945 se define como una organización global, líder y sin fines de lucro para el establecimiento de un estándar de automatización y para proporcionar ayuda a más de 30,000 miembros a nivel mundial y otros profesionales. Las actividades principales de ISA son el desarrollo de estándares, certificación de profesionales de la industria, proveer educación y capacitación, publicación de libros y artículos técnicos, así como organizar la mayor conferencia y exhibición para profesionales de automatización en el hemisferio oeste (ISA-SP100.11, 2006).

El comité ISA SP100 Wireless Systems for Automation, es el encargado de establecer estándares, recomendar prácticas, generar reportes técnicos e información que defina procedimientos para la implementación de sistemas inalámbricos en ámbitos de automatización y control con enfoque a nivel de campo. El comité ISA SP100 realizó un análisis de aplicaciones de comunicación inalámbrica industrial entre dispositivos para clasificar los tipos de comunicaciones. El resultado es una división en seis clases que se muestra en la Tabla VI. Las características principales para la distinción entre las clases son la importancia de los mensajes y el incremento en puntualidad que se refiere a la precisión del tiempo de respuesta de un dispositivo.

Tabla VI. Categorización ISA de Clases de Aplicaciones en Entornos Industriales

Categoría	Clase	Aplicación	Descripción	
Seguridad	0	Acción de emergencia	(Siempre crítica)	Importancia del mensaje ↑ Incremento de puntualidad ↑
Control	1	Control regulador de lazo cerrado	(a menudo crítica)	
	2	Control supervisor de lazo cerrado	(usualmente no crítica)	
	3	Control de lazo abierto	(Humano en el lazo)	
Monitoreo	4	Alarmas	Consecuencia operacional a corto plazo (e.g. mantenimiento basado en eventos)	
	5	Registro, carga/descarga	Sin consecuencias operacionales inmediatas (e.g. recolección de historial, secuencia de eventos, mantenimiento preventivo)	

El ISA-SP100 ha definido los siguientes ejemplos de clases de automatización inalámbrica:

Clase 5: Monitoreo sin consecuencias operacionales inmediatas. Incluye ejemplos sin requerimientos importantes de puntualidad. Algunos, como el registro de secuencia de eventos, requieren alta confiabilidad; otros, como reportes

de cambio lento de los valores o bajo valor económico, no necesitan ser tan confiables ya que la pérdida de muestras consecutivas puede no ser importante.

Clase 4: Monitoreo con consecuencias operacionales a corto plazo. Esta clase incluye alarmas de alto y bajo límite y otro tipo de información que pueda ser revisada por técnicos de mantenimiento. La puntualidad para esta clase de información es típicamente baja, medida en minutos e incluso horas.

Clase 3: Control de lazo abierto. Esta clase incluye acciones donde un operador, más comúnmente que una máquina, "cierra el lazo" entre entrada y salida. Estas acciones pueden incluir apagar una unidad cuando las condiciones lo indiquen. La puntualidad de esta clase de acciones esta en escala humana, medida de segundos a minutos.

Clase 2: Control supervisor de lazo cerrado. Esta clase de control de lazo cerrado usualmente tiene grandes constantes de tiempo, con puntualidad en las comunicaciones medida de segundos a minutos. Un ejemplo es selección de equipo.

Clase 1: Control regulador de lazo cerrado. Estas clases incluyen control de motores y ejes, así como control primario de flujo y presión.

Clase 0: Acciones de emergencia. Esta clase incluye acciones relacionadas con la seguridad que son críticas tanto para el personal como para la planta. La mayoría de las funciones de seguridad son, y serán, desempeñadas a través de

redes alambradas dedicadas para limitar modos de fallo y susceptibilidad a eventos externos o ataques. Algunos ejemplos son control de incendios, apagado de emergencia y dispositivos de seguridad.

El comité ISA-SP100 dividió la investigación en dos grupos de trabajo, para el desarrollo de un protocolo estándar de comunicación para las diferentes clases de aplicaciones definidas. Los grupos de trabajo son el ISA-SP100.11 creado en Abril del 2006 para recomendar un estándar de comunicación inalámbrica para control industrial de lazo y monitoreo, y el ISA-SP100.14 para monitoreo industrial (ISA-SP100.11, 2006).

El principal objetivo del grupo ISA-SP100.11 es proveer conectividad inalámbrica estándar para aplicaciones de clase 1 a 5 con consideraciones para aplicaciones de clase 0. Para esto definirá las especificaciones para las capas OSI, seguridad, administración de red y configuración de dispositivos. El grupo de trabajo generó la primera entrega de lo que nombró el primer estándar inalámbrico de la industria para la industria, el cual, después de ser aceptado por la ISA se pondrá disposición de otras organizaciones de estandarización como IEC para ser utilizado como línea base de otras iniciativas de estandarización. Algunas de las aplicaciones a las que esta dirigida su investigación son: control primario de actuadores directo e indirecto para lazos de proceso en control de flujo, temperatura, presión, etcétera; control inalámbrico de lazo en variables de proceso,

lazos cerrados de control de aceleración para equipo rotativo, etc (ISA-SP100.11, 2006).

Por su parte el grupo de trabajo ISA-SP100.14 como lo define la ISA tiene el propósito de proveer un estándar de conectividad inalámbrica para clases 4 y 5 para dispositivos de complejidad relativamente baja, costo razonable, y bajo nivel de consumo. Además la tasa de datos deberá satisfacer un amplio rango de necesidades que van desde alarmas, registros y carga/descarga. Al igual que su grupo complementario el ISA SP100.14 deberá definir las especificaciones de las capas OSI, de seguridad y administración de la red y sus dispositivos (ISA-SP100.14, 2006).

II.5.1 Requerimientos técnicos.

Por su parte los grupos SP100.11/14 han generado una serie de requerimientos técnicos para pedir la atención y consejo de otros grupos de investigación en el desarrollo del protocolo inalámbrico que desean implementar. La idea principal de estos grupos es revisar las propuestas recibidas y en base a éstas tomar aquellas mejores partes que sea posible ensamblar.

En el siguiente capítulo se realiza una revisión del protocolo ZigBee en base a estos requerimientos técnicos, a manera de lista de verificación para conocer hasta qué punto ZigBee llena los requerimientos establecidos por esta organización.

CAPÍTULO III

ESTANDAR ZIGBEE

El creciente desarrollo de aplicaciones que utilizan redes inalámbricas de sensores, en las que la compatibilidad entre sensores de diversos fabricantes es una necesidad fundamental para la expansión de estas aplicaciones dentro del uso cotidiano, ha generado la búsqueda de un protocolo de comunicación estándar para este tipo de dispositivos, que cada día son más importantes para la investigación y el desarrollo de ambientes de cómputo ubicuo. Las necesidades principales que este tipo de protocolos deben cubrir son: el bajo consumo de potencia, debido a que la instalación y configuración de la red de sensores debe ser lo más sencilla posible; bajo costo tanto para diseño como implementación de la aplicación. Tratando de satisfacer estas necesidades varios se han dado a la tarea de diseñar un protocolo con estas características, algunos de los ejemplos más destacados de éste esfuerzo, debido al tamaño e importancia de la organización, son el comité SP100 de ISA y ZigBee Alliance.

Como ya se mencionó en el capítulo anterior, el comité SP100 se encuentra en la etapa de diseño de un protocolo que ofrecerá como el primer estándar inalámbrico para redes de sensores. Sin embargo ZigBee Alliance lleva un paso adelante y ha comenzado con el desarrollo de una pila de protocolos, llamada

ZigBee, con la finalidad principal de hacer posible el control y monitoreo inalámbrico de productos con base en un estándar abierto de bajo costo y bajo consumo de potencia. Debido al soporte otorgado por el amplio grupo de compañías que forman parte de ésta alianza, a su diseño ligado a aplicaciones existentes y a sus características de estándar abierto y de bajo costo, se espera que ZigBee permita el desarrollo e implementación de muchas aplicaciones en diferentes ámbitos como el hogar, la industria e incluso ambientes médicos. Sin embargo, la alianza ha comenzado el diseño y desarrollo de la pila con un enfoque dirigido a aplicaciones de automatización del hogar y edificios, para posteriormente continuar con el diseño de características necesarias para otros entornos de aplicación.

Dentro de éste capítulo se realiza un análisis detallado del estándar ZigBee con un enfoque dirigido a aquellas características que resultan importantes para su aplicación en ámbitos de monitoreo y automatización industriales.

III.1 ZigBee Alliance

ZigBee Alliance es un conjunto de compañías que se formó con la finalidad de dirigir el desarrollo de la tecnología ZigBee. Algunas de sus tareas principales son el diseño y desarrollo de las capas de red, aplicación y seguridad del protocolo y validación de interoperabilidad entre distintos fabricantes. El objetivo de esta alianza es generar una plataforma inalámbrica óptima, que sirva de estándar para

aplicaciones de monitoreo y control en diversos ámbitos, así como lograr que sea utilizada a nivel mundial, en una gran variedad de dispositivos para uso comercial e industrial.

Algunas de las compañías más importantes que forman parte de esta alianza son: Texas Instruments, Atmel, Ember, Freescale Semiconductor, Integration, Honeywell, Invensys, Mitsubishi Electric, Motorola, Philips, Samsung, Jennic, MeshNetics, Microchip Technology, OKI, Renesas, Silicon Laboratorios, Itron, NEC, NXP, STMicroelectronics, Eaton, Honeywell, Johnson Controls, LG, Schneider Electric, Siemens, etc.

Debido a que esta asociación de compañías es ya muy grande y continúa creciendo, las probabilidades de adopción de este protocolo por parte de la industria, como un estándar para el desarrollo de productos que permitan dar un paso adelante en la creación de ambientes de cómputo ubicuo, parecen ser bastante grandes. Además, asegura a desarrolladores de sistemas más complejos que utilicen el estándar ZigBee de comunicación, un amplio soporte para su uso y compatibilidad con una gran variedad de sistemas de otros fabricantes.

Este amplio soporte, otorgado por el conjunto de empresas que respaldan el desarrollo y aplicación de ZigBee, es la razón principal para tomarlo como objeto de estudio en esta investigación Puede decirse que existe una gran cantidad de soluciones que buscan atacar el mismo nicho de aplicaciones que ZigBee, sin

embargo, no cuentan con las dos características que distinguen a ZigBee: es un estándar abierto y tiene un amplio soporte.

III.2 Principales características

Desde el punto de vista de ZigBee Alliance, se ha buscado dar a ZigBee una amplia promoción como la solución para el desarrollo de aplicaciones en muy diferentes ámbitos como son: consumibles electrónicos, automatización del hogar y edificios comerciales, automatización industrial, instrumentación médica y monitoreo ambiental. Sin embargo el enfoque inicial principal para el desarrollo del estándar ha sido la automatización del hogar. Con base en esto se han tomado una serie de decisiones importantes sobre las características principales del protocolo.

En primer lugar ZigBee está diseñado con base en el estándar IEEE 802.15.4 para las capas física y de acceso al medio; este diseño exige un bajo consumo de potencia en los dispositivos utilizados y por lo tanto garantiza una vida más larga a las baterías, que como se sabe, es una necesidad intrínseca a la mayoría de las aplicaciones de sensores inalámbricos. Algunas otras características que ZigBee adquiere debido a su cimentación en el protocolo IEEE 802.15.4 son una tasa de datos baja, rango de distancia corto y una interfaz diseñada para dispositivos con limitaciones en el consumo de energía, de CPU y de memoria. De igual manera el

hecho de utilizar un estándar permite asegurar la coexistencia en una misma frecuencia de diferentes marcas de dispositivos.

En el diseño realizado por ZigBee Alliance para las capas superiores, se destacan los dos tipos de enrutamiento: árbol y malla. Aunado a esto se cuenta con tres tipos de dispositivos, dependiendo de los servicios de capa red que se desea que realicen. La posibilidad de elegir entre estas opciones ofrece mayor libertad a los diseñadores de aplicaciones, sin embargo, debe tomarse en cuenta el costo en memoria y desempeño al elegirlas.

Otra de las características principales que podemos encontrar en el diseño de este protocolo es la creación de un marco de trabajo para aplicaciones. ZigBee Alliance busca no solamente diseñar un protocolo de comunicación, sino permitir el desarrollo de aplicaciones estandarizadas sencillas y de uso cotidiano de una manera más rápida. Por esta razón ha generado un conjunto de bibliotecas y perfiles estándar para la creación de dispositivos utilizados con frecuencia en los ámbitos de aplicación de ZigBee. Debido a esta característica, no puede considerarse a ZigBee como un simple conjunto de comandos para la comunicación entre dispositivos sino como un marco de trabajo que permite la creación de dispositivos estandarizados en los que puede asegurarse su interoperabilidad con otros fabricantes y dispositivos propietarios que podrán ser diseñados a la medida de las necesidades de los usuarios.

Hasta este momento las pruebas de interoperabilidad entre dispositivos estándar se han realizado únicamente para el ámbito de automatización del hogar, que como se mencionó antes ha sido el principal enfoque de ZigBee Alliance.

III.3 Arquitectura ZigBee

La arquitectura de ZigBee mostrada en la Figura 4 tiene un diseño en capas, cada una de las cuales ofrece servicios a la capa superior inmediata, comunicándose a través de puntos de acceso de servicios (SAP, por sus siglas en inglés) que se distinguen como servicios de entidad de datos (Data Entity) o servicios de entidad de manejo (Management Entity). La entidad de datos ofrece únicamente el servicio de transmisión de datos entre una capa y otra, y la entidad de manejo permite el envío de comandos para el control y administración de otros servicios en las capas.

Como se mencionó anteriormente, las capas física y de acceso al medio están definidas de acuerdo al estándar 802.15.4, por lo tanto, los puntos de acceso hacia sus entidades están definidos por este mismo protocolo. Sobre la base de estas dos capas, el estándar ZigBee define la capa de red (NWK) como la encargada de definir mecanismos como la formación de la red y administración de direcciones, enrutamiento, aplicación de seguridad y descubrimiento de servicios y dispositivos.

Sobre la capa de red se define la capa de aplicaciones conformada por tres elementos, la subcapa de soporte de aplicaciones (APS), el objeto del dispositivo ZigBee (ZDO) con su plano vertical de manejo, y el marco de trabajo de la aplicación que contiene a los objetos de aplicación definidos por el usuario. La función principal de la APS es ofrecer una interfaz entre la capa de red y las capas superiores, a través de las entidades de datos y de servicios (APSDE y APSME).

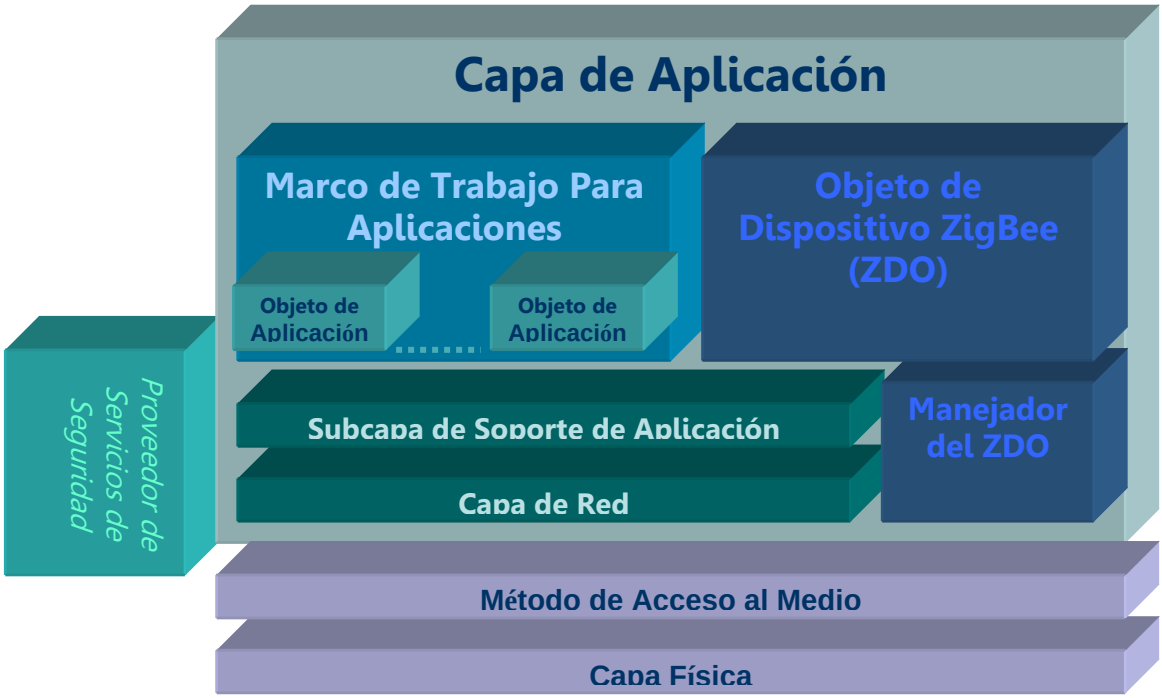


Figura 4. Arquitectura ZigBee

A continuación se realiza un análisis más detallado de los elementos principales de la arquitectura del protocolo ZigBee de acuerdo a su descripción en la especificación del estándar, con la finalidad de obtener un conocimiento

profundo tanto de aquellas características que podrán resultar útiles en ámbitos de control y automatización industrial como de aquellas que podrían mermar su capacidad para enfrentar las necesidades de éste tipo de aplicaciones. Para realizar este análisis se tomará como guía el estudio por capas del protocolo, resaltando las características principales, ofreciendo una explicación detallada de su funcionamiento y las ventajas y desventajas que aportan al protocolo.

III.3.1 Capa de red (NWK)

La capa de red funciona como la interfaz entre el APS y la subcapa MAC IEEE 802.15.4, pero además, se encarga de varios servicios referentes a la administración de la red, el enrutamiento y la seguridad. En ZigBee, a nivel de la capa de red existen tres tipos de dispositivos, cada dispositivo tiene capacidad para ofrecer diferentes servicios de la capa de red.

El Coordinador ZigBee (ZC) está definido como un dispositivo de funcionalidad completa (FFD o Full Function Device, en inglés) para la capa MAC. Es el encargado de formar la red ZigBee, es decir, asigna un identificador a la red (PAN ID) con el cuál la red formada se distinguirá de cualquier otra red ZigBee que exista dentro del mismo canal de transmisión, por lo tanto el ZC debe ser el único en su tipo dentro de la red. Esta funcionalidad es la que lo distingue de un Enrutador ZigBee (ZR, por sus siglas en inglés), también definido como dispositivo de funcionalidad completa (FFD) para capa MAC. Al igual que el ZC tiene capacidad

para asignar direcciones lógicas, permitir que otros dispositivos se unan y separen de la red, enrutar paquetes o bien simplemente transferirlos; sin embargo no puede formar una red, solamente unirse a una ya existente. El tercer tipo es el Dispositivo Terminal ZigBee (ZED, por sus siglas en inglés) es el más sencillo de todos, debido a que se define como dispositivo de funcionalidad reducida (RFD, Reduced Function Device) para la capa MAC, únicamente puede unirse y separarse de una red y transferir paquetes, no tiene capacidad para enrutar paquetes ni asignar direcciones lógicas.

Para proveer sus servicios la capa de red cuenta con dos entidades la de datos (NLDE, Network Layer Data Entity) y la de administración (NLME, Network Layer Management Entity). La NLDE se encarga de los siguientes servicios:

- Generar el PDU (Packet Data Unit) de la capa de red.
- Enrutamiento específico de la topología
- Asegurar la autenticidad y confidencialidad de una transmisión.

En cambio la NLME provee servicios referentes al manejo y administración de la capa de red, específicamente ofrece los siguientes servicios:

- Configuración de un dispositivo nuevo en la red.
- Establecimiento de la red.
- Unión, reunión y separación de la red.
- Asignación de direcciones.

- Descubrimiento de vecinos.
- Descubrimiento de rutas.
- Control de recepción y sincronización de la subcapa MAC
- Enrutamiento.

Para hacer posible la ejecución de estos servicios, es necesario un importante elemento de la capa de red; la Base de Información de la Capa de Red (NIB, Network Information Base, en inglés) ésta funciona como la base de datos que contiene toda información importante para el establecimiento y administración de la red. La información contenida en la NIB, se refiere a todas las constantes y atributos que cada dispositivo debe tener definidos para formar parte de la red y ser capaz de comunicarse en forma apropiada. Algunos ejemplos de estas constantes y atributos son: nwkcCoordinatorCapable (define si el dispositivo es coordinador de la red), nwkcRouteDiscoveryTime (tiempo máximo para que caduque el descubrimiento de una ruta), nwkMaxChildren (el número máximo de hijos[3] del dispositivo), etc.

Entonces, con base en algunas constantes y atributos predefinidos en la NIB y a través de los servicios ofrecidos por la capa de red se llevan a cabo varios procesos importantes para el establecimiento, configuración y mantenimiento de una red. De igual manera, los cambios generados durante la vida de la red, y para su mantenimiento son reflejados en la NIB.

[3] En este caso se llama hijos de un dispositivo a todos aquellos dispositivos que se unen a la red y reciben una dirección lógica a través de él.

A continuación se describen algunos de los procesos más importantes para el establecimiento, configuración y mantenimiento de la red.

- Formación de la Red.
- Unión a la red.
- Asignación de direcciones.
- Enrutamiento.

III.3.1.1 Formación de la Red.

El proceso de formación de la red es realizado por el coordinador (ZC). En términos generales el ZC realiza una detección del nivel de energía en varios canales para elegir aquel que tenga el menor nivel de interferencia para la comunicación de la red. También pude establecerse la formación de la red en un canal determinado, en cuyo caso esta detección de energía no es necesaria. La lista de canales disponibles será primero ordenada por el nivel de interferencia y después por el número de redes ZigBee establecidas en él. Una vez elegido el canal, debe revisarse el PAN ID de las redes ZigBee existentes para encontrar un identificador único propio, si esto no es posible la formación de la red deberá notificarse como no exitosa a las capas superiores del protocolo. Si el identificador de la PAN es encontrado, el nodo adquirirá la dirección lógica 0x0000 notificando el resultado de la formación de la red a las capas superiores.

III.3.1.2 Unión a la red.

Los únicos dispositivos que permiten la unión de un nodo a la red son el coordinador o los enrutadores. Un dispositivo terminal no puede permitir la unión de un nuevo nodo. Además para permitir la unión del nuevo nodo, al menos uno de los enrutadores o bien el coordinador debe tener su parámetro PermitDuration diferente de 0x00. Existen dos maneras de unir un nodo a la red: por medio del proceso de asociación de la MAC, o bien guardando la información del nodo directamente en la tabla de vecinos del dispositivo padre elegido previamente.

III.3.1.3 Asignación de direcciones.

Cada dispositivo ZigBee recibe una dirección lógica de 16 bits al unirse a la red. Las direcciones son asignadas de acuerdo a un esquema distribuido que permite que cada padre reciba un sub-bloque finito y único de direcciones. El ZC determina el número máximo de hijos que cualquier nodo padre de su red podrá tener, para esto se define desde un principio el número máximo de hijos enrutadores y el número máximo de hijos que serán dispositivos terminales.

III.3.1.4 Enrutamiento.

El protocolo ZigBee ofrece tres tipos de topologías lógicas: estrella, árbol y malla. La topología estrella consiste en la formación de la red utilizando un nodo coordinador como encargado de formar la red y permitir la unión del resto de los

nodos, que para esta topología serán nodos terminales. En este caso, los dispositivos terminales carecen de capacidades de enrutamiento y por lo tanto se comunican entre ellos a través del coordinador. Esta topología puede llevarse a cabo utilizando nodos enrutadores, sin embargo sus capacidades de enrutamiento no serían utilizadas en todo su potencial. En la Figura 5 se observa la formación obtenida en una red de topología estrella. Las características principales de estas redes son una profundidad máxima de 1 y la ausencia total de comunicación directa entre los dispositivos terminales.

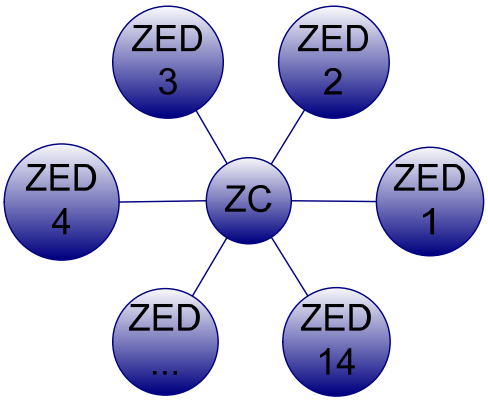


Figura 5. Topología estrella

En el caso de las redes de topología árbol, la ventaja principal que se obtiene es la extensión de la red haciendo uso de las capacidades de enrutamiento jerárquico de los nodos enrutadores, de esta manera es posible generar una red como la que se observa en la Figura 6 y por lo tanto multiplicar la distancia de envío de los mensajes.

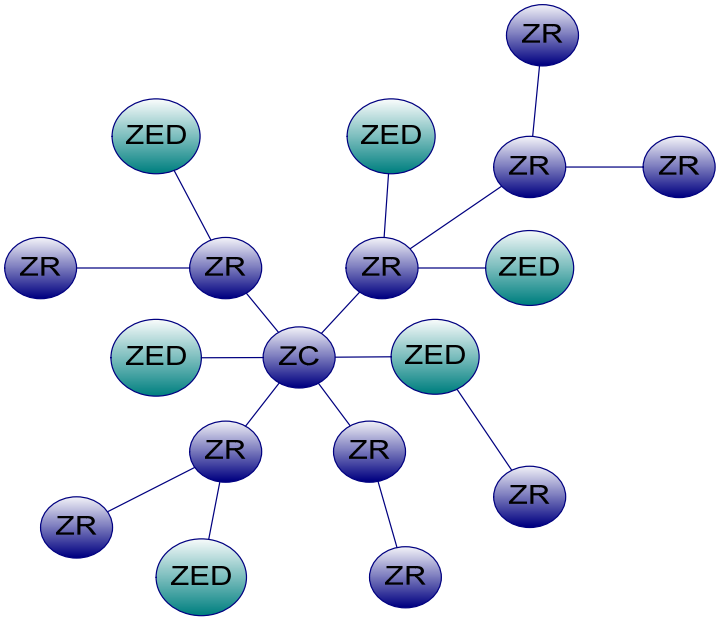


Figura 6. Topología arbol

En este tipo de redes no es posible la comunicación directa entre nodos que no tengan una relación padre-hijo, los mensajes entre nodos de diferentes niveles viajan a través de la jerarquía establecida por la topología. De esta manera, un mensaje enviado a un nodo de la misma profundidad deberá ser enviado al nodo padre para que este lo entregue al hijo correspondiente. Otra ventaja más de esta topología es que a pesar de ser capaz de lograr el enrutamiento de paquetes, no se tiene el gasto extra de memoria y procesamiento en descubrimiento de rutas. Sin embargo, el ahorro de recursos para el descubrimiento de rutas limita las capacidades de recuperación de la red en caso del fallo de algún dispositivo. Por lo tanto las redes formadas con esta topología son consideradas más vulnerables a los fallos y de baja robustez.

Para el caso de las redes de topología malla, se hace uso del enrutamiento malla a través del descubrimiento de rutas. En esta topología los nodos enrutadores tienen capacidad de comunicarse con cualquier nodo que se encuentre dentro del radio de recepción y transmisión efectivo de su antena, de esta manera un enrutador puede comunicarse con otro directamente, aunque su posición en la jerarquía de la red tenga una distancia de varios saltos. Las ventajas principales de este tipo de topología son la posibilidad de descubrir rutas más directas o con menos saltos, para el envío de mensajes, y una mayor posibilidad de recuperar la comunicación entre dispositivos, aún cuando uno de los nodos intermediarios sufra algún daño. Por otro lado estas ventajas tienen un costo extra en memoria y procesamiento, debido a la necesidad del mantenimiento de tablas de enrutamiento y la implementación de funciones para el descubrimiento de rutas.

III.3.2 Capa de aplicación

Como se mencionó antes, la capa de aplicación está formada por tres elementos principales, la Sub-capa de Soporte de Aplicación (APS, Application Support Sublayer), los Objetos del Dispositivo ZigBee (ZDO, ZigBee Device Object) y el Marco de Trabajo para los objetos de los dispositivos diseñados por el usuario. Conocer estos tres elementos nos permite comprender mejor la filosofía con que fue diseñado el protocolo y observar las ventajas ofrecidas por su estandarización.

III.3.2.1 Subcapa de Soporte de Aplicación (APS)

El APS funciona como interfaz entre cualquier objeto de la capa de aplicación, ya sea que esté definido para el dispositivo ZigBee o bien para algún dispositivo de la aplicación del usuario. Para lograr esto el APS proporciona un conjunto determinado de servicios a partir de sus dos entidades, la de datos (APSDE) y la de manejo (APSME).

El APSDE provee los siguientes servicios:

- Generar el PDU de la capa de aplicación (APDU)
- Enlazamiento de dispositivos con base en los servicios ofrecidos por sus objetos. El APSDE debe encargarse de enviar los mensajes entre los dispositivos que se encuentren enlazados a través de este servicio.
- Filtrado de direcciones de grupo
- Transporte confiable de paquetes.
- Rechazo de dúplicas de mensajes enviados desde la aplicación.
- Fragmentación y reensamble de mensajes mayores al tamaño máximo de carga útil de la capa NWK.

Por su parte el APSME ofrece los siguientes servicios:

- Administración de enlaces.
- Administración de la base de datos de los objetos pertenecientes a la subcapa de soporte de aplicación (AIB, Application Information Base).

- Autenticación de las relaciones con otros dispositivos a través de llaves de seguridad.
- Administración de la pertenencia de los dispositivos a grupos.

A través de sus entidades de servicios (APSDE y APSME), la subcapa de soporte de aplicación permite la comunicación entre una capa superior y la de red, sin embargo, a diferencia del APSDE, el APSME solo permite el uso directo de dos primitivas de la capa de red, solo se puede acceder al resto de las primitivas del NLME a través del ZDO.

III.3.2.2 Marco de trabajo de la aplicación.

Se refiere al ambiente dentro del cual se albergan los objetos de los dispositivos ZigBee. Para generar este marco de trabajo se requiere definir los siguientes elementos:

- Perfil de aplicación.
- Biblioteca de Clusters.

III.3.2.2.1 Perfil de aplicación

El perfil de la aplicación consiste en la descripción de los dispositivos que se utilizarán y la distribución de la funcionalidad de la aplicación entre estos dispositivos. El hablar de dispositivos en ZigBee, se refiere a un conjunto de

objetos definidos para ofrecer la funcionalidad necesaria en cierta área de aplicación. Para comprender mejor la filosofía de los perfiles de aplicación de ZigBee, debe tomarse en cuenta que éste protocolo está diseñado para ofrecer interoperabilidad entre diferentes marcas de manufactura. Por lo tanto, al definir un perfil de aplicación, se definen los dispositivos que pueden ser utilizados dentro de ésta aplicación y los comandos con que se comunicarán, de manera que dos dispositivos para un mismo perfil de aplicación hechos por compañías diferentes deben ser capaces de comunicarse sin problemas.

En el caso de que un fabricante desee que sus dispositivos tengan la posibilidad de ser utilizados en forma estándar, debe pedir un número de perfil asignado por ZigBee Alliance. De esta manera su perfil será agregado a la descripción del estándar al igual que los dispositivos y clusters que utilice.

Para explicar con mayor detalle las características de un perfil de aplicación podemos tomar el Perfil de Automatización del Hogar (HA, Home Automation) del estándar ZigBee. Este perfil clasifica los dispositivos en categorías según el área de automatización en que se utilicen, a continuación se nombran algunos ejemplos de dispositivos según ésta clasificación:

- Genéricos: Interruptor encendido/apagado, Interruptor de Control de Nivel, Control de Escena, etc.
- Alumbrado: Luz Encendido/Apagado, Luz de Niveles, Interruptor de Niveles, etc.

- Encierro: Sombra, Control de Ensombrecimiento, etc.
- Calefacción, Ventilación y Aire Acondicionado (HVAC): Termostato, Unidad de Calefacción/Enfriamiento, Detector de temperatura, etc.
- Sistema de Alarma de intrusos: Control Indicador de Equipo, Zona, Dispositivo de Alarma, etc.

Entonces, el perfil de aplicación debe definir los dispositivos que serán utilizados en el área de aplicación. La definición de los dispositivos consiste en dos elementos:

- Número de identificador del dispositivo.
- Clusters utilizados.

III.3.2.2.2 Clusters

Los clusters son la definición de una funcionalidad distribuida en dos dispositivos, por lo tanto un cluster puede ser implementado como servidor o como cliente. De ésta manera la implementación cliente de un cluster en un dispositivo puede realizar la petición de un servicio a la implementación servidor de ese cluster en otro dispositivo. Para mayor claridad se ofrece el siguiente ejemplo:

De acuerdo a la definición del dispositivo Interruptor Encendido/Apagado en el Perfil de Automatización del Hogar, éste dispositivo implementa el cluster cliente Encendido/Apagado. Por otro lado el dispositivo Luz Encendido/Apagado

implementa el cluster servidor Encendido/Apagado. De ésta manera, un nodo inalámbrico programado como Interruptor Encendido/Apagado ZigBee puede enviar una petición para encender o apagar una Luz Encendido/Apagado ZigBee. Esta petición será atendida sin importar el tipo de hardware utilizado siempre y cuando el protocolo ZigBee sea utilizado apropiadamente. Como puede observarse, la funcionalidad distribuida es el encendido y apagado de una luz, el lado cliente realiza la petición y el servidor la ejecuta encendiendo o apagando una luz a la que se encuentre conectado.

La definición del cluster consiste en el conjunto de comandos que pueden ser enviados por el cliente y su efecto en el servidor. Por esta razón se dice que indican el sentido en el flujo de datos en el dispositivo.

III.3.2.2.3 Puntos Terminales (Endpoints)

El Punto Terminal es un número que identifica a los diferentes dispositivos de aplicación que pueden residir en un nodo. Cada nodo puede tener hasta 240 puntos terminales del 0x01 al 0xF0. El Punto Terminal 0x00 está definido para el dispositivo ZigBee. El punto terminal 0xFF se considera un *broadcast* para todos los puntos terminales que se encuentren activos. Y los valores del 0xF0 al 0xFE se encuentran reservados.

III.3.2.3 Dispositivo de Objetos ZigBee (ZDO)

El dispositivo de objetos ZigBee define una clase básica de funcionalidad que provee la interfaz entre los objetos de la aplicación, el dispositivo del perfil, la subcapa de soporte de aplicación y varios servicios de la capa de red. Sus principales tareas son:

- Inicializar la subcapa de soporte de aplicación, la capa de red y el proveedor de servicios de seguridad.
- Utilizar la información de configuración para determinar e implementar el descubrimiento de dispositivos y servicios y la administración de la red, la seguridad y el enlace de dispositivos.

Puede decirse que el objetivo final del diseño del ZDO es la creación de un administrador de las funciones básicas de cualquier dispositivo de aplicación ZigBee, que además funcione como interfaz de diferentes funcionalidades del protocolo.

III.3.2.4 Enlace de dispositivos.

A través del enlace de dispositivos, es posible que cualquier dispositivo ZigBee designe una dirección destino para todos los paquetes que se generen desde un punto terminal dado y con un cluster específico. Existen dos formas de realizar el enlace de dispositivos:

Enlace entre dos dispositivos. Esto se da cuando ambos dispositivos generan en su tabla de enlace, una entrada con la dirección destino del otro dispositivo. Puede decirse que cada dispositivo está conciente de la existencia del otro y genera un comando para requerir la creación de una entrada en la tabla de enlaces del otro dispositivo que describa su enlace con éste.

Enlace de dispositivos terminales. En este caso los dispositivos generan una petición al coordinador, para que determine si existe otro dispositivo que cuente con clusters de entrada que correspondan apropiadamente con los clusters de salida que él tiene. El proceso es el siguiente: el dispositivo A envía una petición al coordinador para un enlace de dispositivos terminales, dentro de éste paquete envía la lista de clusters de salida con que cuenta para realizar el enlace. Si en un tiempo determinado para el enlace, el dispositivo B envía una petición al coordinador, para un enlace de dispositivos terminales con una lista de cluster de salida donde al menos uno tiene el mismo identificador que algún cluster de la lista de entrada del dispositivo A o viceversa. Entonces el nodo coordinador enviará una petición de enlace a cada uno de los dispositivos, para que generen en su tabla de enlaces una entrada que contenga la dirección del otro.

La finalidad principal del proceso de enlace de dispositivos es poder encontrar otros dispositivos que puedan ofrecer la funcionalidad necesitada aún si no pueden comunicarse directamente. El principal problema de éste proceso es que se encuentra centralizado en el coordinador, si el coordinador falla no podrá

realizarse el enlace de dispositivos terminales. Además esto limita en tiempo la configuración de una red, debido a que el coordinador solo podrá atender un número determinado de enlaces cada cierto tiempo.

III.3.2.5 Grupos

El protocolo ZigBee permite asociar puntos terminales a direcciones de grupos y por lo tanto se define un tipo de paquete con dirección de grupo. Para lograr esto, cada dispositivo debe ser capaz de asociar sus puntos terminales a direcciones de grupos con comandos del APS, esta asociación se establece en una tabla de grupos que debe ser consistente entre la subcapa de soporte de aplicación y la de red. Una característica importante de los enlaces en ZigBee, es que pueden hacerse enlaces con direcciones de grupos, no solamente con direcciones de dispositivos.

III.3.2.6 Direccionamiento.

Debido a que ZigBee ofrece dos tipos de direcciones (NWK y MAC), envío de mensajes *broadcast*, *multicast* y *unicast*, y además cuenta con capacidad para formar grupos y enlaces, es necesario que se utilicen diferentes tipos de direccionamiento reconocidos por la capa de APS para determinar el tipo de paquete que ha llegado.

Como ya se mencionó cada nodo ZigBee cuenta con dos direcciones, la dirección MAC o física, consiste en un número único de 64bits para identificación del hardware utilizado, esta dirección equivale a la dirección MAC con que cuentan las tarjetas de red de las computadoras. Por otro lado cuando un nodo ZigBee se une a una red adquiere una dirección de red que consiste en 16bits; esta dirección depende del tipo de nodo (enrutador o dispositivo terminal) y le es entregada por parte del padre al que se unió. El nodo coordinador siempre forma la red y por lo tanto toma la dirección 0x0000.

En un paquete ZigBee existen tres partes importantes relacionadas con el direccionamiento.

- Direcciones de la capa MAC.
- Direcciones de la capa de red.
- Modo de direccionamiento de la subcapa de soporte de aplicación.

En el caso de que un paquete necesite más de un salto para llegar a su destino, la capa de red mantiene el valor de la dirección destino mientras la dirección de la capa MAC cambia para indicar el siguiente nodo destino en la ruta. En el caso de una dirección *broadcast*, los nodos enrutadores que lo reciben deben repetirlo para que pueda llegar a todos los nodos de la red.

Mientras que la capa MAC y la de red se encargan de filtrar los paquetes que están dirigidos al dispositivo. La subcapa de soporte de aplicación debe hacerse

cargo de reconocer si está dirigido a uno de sus puntos terminales o bien a un grupo del que alguno de sus puntos terminales forme parte. Esto sucede cuando un paquete viaja por el aire y es recibido por la capa física y dirigido hacia la aplicación. Sin embargo, cuando una aplicación requiere enviar un mensaje, también debe indicar el tipo de dirección que está usando. Por ejemplo, en el caso de tratarse de un enlace la subcapa de soporte de aplicación busque y agregue la dirección del enlace, si esta existe. A continuación se explican con más detalle los tipos de direccionamiento utilizados al enviar un mensaje desde la capa de aplicación.

Modo de direccionamiento para enlaces (0x00). Cuando la subcapa de soporte de aplicación recibe un mensaje desde una capa superior con este modo de direccionamiento, significa que si existe la tabla de enlaces, entonces debe verificar todas aquellas entradas que contengan el punto terminal fuente indicado en el mensaje. Para cada entrada encontrada deberá generar un mensaje tomando la dirección destino y el modo de direccionamiento de la tabla de enlaces.

Modo de direccionamiento para grupos (0x01). Al recibir un mensaje desde una capa superior, con este modo de direccionamiento, la subcapa de soporte de aplicación generará un mensaje con dirección broadcast y en la trama de APS especificará el modo de entrega como (0x03) y la dirección de grupo a la que va dirigida el mensaje. En el caso de que la subcapa de soporte de aplicación reciba un mensaje desde la capa de red con un valor 0x03 en el modo de entrega,

tomará la dirección de grupo de la trama APS del mensaje y buscará en la tabla de grupos aquellos puntos terminales que sean parte de éste. Si existe alguno, la subcapa dirigirá el mensaje a esos puntos terminales para que los objetos de aplicación correspondientes lo procesen en forma apropiada.

Modo dirección de 16bits (0x02). Este tipo de direccionamiento sólo puede utilizarse en los casos en que se tiene las direcciones de red y del punto terminal del nodo al cual va dirigido. Al recibirlo, la subcapa de soporte creará el mensaje utilizando los valores especificados para estos parámetros.

Modo dirección de 64bits (0x03). En este caso, la subcapa de soporte recibe una dirección de 64bits, con la cual deberá encontrar la dirección de 16bits correspondiente en la base de información de red (NIB). Sólo en caso de encontrarla, formará un mensaje con modo de entrega *unicast* y especificará la dirección de 16bits encontrada en la base de información de red.

III.3.2.7 Descubrimiento de dispositivos

Se le nombra de esta manera al proceso mediante el cual un dispositivo ZigBee puede encontrar otros dispositivos ZigBee. Es posible realizar este proceso a través de dos comandos del ZDO.

Petición de la dirección de 16bits. En este caso se realiza la búsqueda de un dispositivo a través de su dirección de 64 bits, la cual es enviada en un mensaje

broadcast llamado NWK Address Request. Si el dispositivo con la dirección de 64 bits recibe el mensaje, entonces debe responder enviando su dirección de 16 bits en un mensaje *unicast* llamado NWK Address Response.

Petición de la dirección de 64bits. En este caso se realiza la búsqueda de un dispositivo a través de su dirección de 16 bits, la cual es enviada en un mensaje *unicast* llamado IEEE Address Request. Si el dispositivo con la dirección de 16 bits recibe el mensaje, entonces debe responder enviando su dirección de 64 bits en un mensaje *unicast* llamado IEEE Address Response.

III.3.2.8 Descubrimiento de servicios.

Mediante este proceso, es posible descubrir las capacidades de cada dispositivo ZigBee disponible en la red. Para esto puede realizarse una petición de comparación de servicios *broadcast* o *unicast* a cada punto terminal de un dispositivo ZigBee. En este caso se utiliza un comando del ZDO llamado Match Descriptor Request. Al utilizar este comando el dispositivo que lo envía especifica un identificador de perfil, la lista de clusters de entrada y de salida junto con sus tamaños para que estas listas sean verificadas por aquellos dispositivos que reciban el comando. Al contestar este comando con un Match Descriptor Response, el nodo que responde, en caso de encontrarlos, debe especificar la lista de puntos terminales que coincidieron con los clusters especificados.

III.3.3 Servicios de seguridad

El diseño de seguridad en ZigBee responsabiliza a cada una de las capas por la seguridad de su trama. De ésta manera, la capa que genere un paquete debe asegurarse de que sea protegido en forma apropiada. Sin embargo las tareas de seguridad están repartidas entre la subcapa de soporte de red, la capa de red y el dispositivo de objetos ZigBee. En general la subcapa de soporte de red se encarga de ofrecer servicios para establecimiento y administración de las llaves. El dispositivo de objetos ZigBee por su parte administra las políticas de configuración de seguridad de los dispositivos y la capa de red al igual que la subcapa de soporte de aplicación se encarga de asegurar su trama al transmitir, de acuerdo al nivel de seguridad especificado.

III.3.3.1 Llaves

Existen tres tipos de llaves en los dispositivos ZigBee: llave de enlace, llave de red y llave maestra. La comunicación entre los dispositivos ZigBee puede basarse en la llave de enlace o en la de red. En el caso de que la comunicación sea *unicast* se comparte una llave de enlace de 128 bits entre los dos dispostivos, en cambio para el caso de comunicación *broadcast* se hace uso de una llave de red de 128 bits, que todos los dispositivos dentro de la red deben compartir. Existen dos tipos de llave de red: estándar y de alta seguridad. Dependiendo el tipo de llave de

red utilizado es posible controlar el modo en que la llave es distribuida y la inicialización de los contadores de tramas.

Las llaves de enlace pueden ser adquiridas por los dispositivos de tres maneras: por establecimiento de llave, transporte de llave o bien pre-instalación. En cambio la llave de red puede ser adquirida únicamente por transporte o pre-instalación.

En el caso de que la llave de enlace sea adquirida por establecimiento de llave, es necesario que el dispositivo adquiera primero una llave maestra a través de los procesos de transporte de llave o pre-instalación.

III.3.3.2 Seguridad en la subcapa de soporte de aplicación.

La subcapa de soporte de aplicación está encargada de manejar el aseguramiento de los paquetes provenientes de la aplicación para lo cuál realiza las siguientes tareas:

- Proteger su trama.
- Permite especificar el tipo de llave de seguridad que se utilizará como base.
- Provee los siguientes servicios a las aplicaciones y al dispositivo de objetos ZigBee.
- Establecimiento de llave

- Transporte de llave
- Actualización de llave
- Destitución de dispositivos
- Requisición de llave
- Cambio de llave
- Autentificación de entidad

III.3.3.3 Establecimiento de llave.

Con este procedimiento es posible derivar una llave de enlace secreta, compartida por dos dispositivos, a partir de la información entregada a los dos dispositivos. Para realizar este proceso deben cumplirse los siguientes pasos:

- Entrega de información efímera.
- Derivación de la llave de enlace a partir de la información efímera.
- Confirmación de que la llave de enlace fue generada correctamente.

En el caso de utilizar el protocolo de establecimiento de llave con llave simétrica la llave de enlace es derivada de una llave maestra.

III.3.3.4 Transporte de llave.

Este servicio permite que un dispositivo ZigBee haga llegar una llave maestra, de enlace o de red en forma segura o no segura a otros dispositivos. El

transportar una llave en forma no segura, permite dar a un dispositivo una llave inicial para comenzar la comunicación segura, sin embargo esto solo puede ser utilizado en aplicaciones con seguridad baja, debido a que se compromete por unos instantes la seguridad de la red al enviar una llave de comunicación en un paquete no cifrado.

III.3.3.5 Actualización de dispositivo.

Con este servicio un dispositivo puede comunicar a otro cuando sucede un cambio en el estado de un tercer dispositivo. Por ejemplo en el caso de que un nodo enrutador permita a otro nodo unirse a la red, debe utilizar este servicio para hacer saber al dispositivo central de seguridad sobre la unión del nuevo nodo.

III.3.3.6 Destitución de dispositivo.

En los casos en que el dispositivo central de seguridad detecte que se ha unido un dispositivo no permitido a la red, puede utilizar este servicio para requerir que el dispositivo padre del nuevo nodo lo remueva de la red. Para esto deberá utilizar el servicio de destitución de dispositivo.

III.3.3.7 Cambio de llave.

Cómo una medida extra de seguridad se recomienda que la llave de cifrado utilizada sea modificada cada cierto tiempo para dificultar su captura por agentes

dañinos, en éstos casos, después de transportar la nueva llave que se desea utilizar, el dispositivo central de seguridad puede requerir mediante un mensaje *unicast* o *broadcast* que alguno o todos los nodos de la red cambien la llave de seguridad que utiliza la red. Después de hacer esto el dispositivo central de seguridad debe cambiar su llave también, para poder comunicarse con los otros nodos. Si un dispositivo cuenta con más de una llave, puede utilizar cualquiera para leer los mensajes que llegan, pero solamente emitirá mensajes cifrados con la llave activa.

III.3.3.8 Autentificación de entidad.

Mediante este proceso es posible sincronizar la información con otro dispositivo mientras se le autentifica mediante una llave compartida.

III.3.3.9 Coordinador ZigBee en una Red Segura.

Dentro de una red con seguridad, el coordinador ZigBee tiene a su cargo algunas tareas específicas como son:

- Configurara el nivel de seguridad de la red.
- Ser el dispositivo central de seguridad por defecto, o bien la dirección del mismo.

III.3.3.10 Dispositivo central de seguridad.

Este dispositivo debe residir en un nodo considerado seguro para la red, generalmente y por defecto se utiliza al coordinador de la red como dispositivo central de seguridad. Este dispositivo debe realizar las siguientes tareas:

- Distribuir las llaves para aplicaciones de red o punto a punto.
- Debe ser configurado para operar en modo de seguridad alta o estándar.
- Establecer las llaves de aplicación punto a punto enviando llaves maestras para el procedimiento o bien enviando llaves de enlace directamente.

III.3.3.10.1 Modo de seguridad alta.

Diseñado para aplicaciones que requieren un nivel de seguridad superior al estándar este modo de seguridad permite el mantenimiento de listas de dispositivos, llaves maestras, llaves de enlace y llaves de red dentro del dispositivo central de seguridad. De esta manera es posible un control y administración más riguroso de la red. Sin embargo, debido a la necesidad de espacio para almacenar toda la información necesaria, el costo en memoria de este modo de seguridad es mucho mayor y aumenta conforme crece el tamaño de la red.

III.3.3.10.2 Modo de seguridad estándar.

Este modo está dirigido a aplicaciones residenciales en las cuales el nivel de seguridad requerido es menor, por lo que el dispositivo central de seguridad sólo necesita mantener una llave de red estándar y las políticas de control de admisión de dispositivos. Debido a que el dispositivo central de seguridad no necesita mantener listas de dispositivos ni llaves de seguridad, sus requerimientos de memoria no crecen con el tamaño de la red.

III.3.3.11 Unión en una red segura.

A diferencia de la unión dentro de una red no segura, cuando un nodo sin la llave de cifrado se une a una red con seguridad, o bien ha perdido alguna actualización de llave y necesita volver a pedirla, debe realizarse el procedimiento descrito en el siguiente párrafo.

La unión a la red es la misma, se envían los paquetes de la capa MAC necesarios para requerir la asociación a la red y el dispositivo se une al nodo padre. Sin embargo, hasta este momento el nodo se encuentra unido pero no autentificado. Por lo tanto ningún paquete o llave debe ser enviado al mismo hasta que el proceso de autentificación haya terminado.

III.3.3.12 Autentificación

En el momento de recibir una confirmación de unión de un nuevo nodo, el nodo padre debe enviar hacia el dispositivo central de seguridad un mensaje de actualización de dispositivo para informarle sobre el nodo nuevo que se ha agregado a la red.

Existen varios factores que afectan la autentificación de un dispositivo, por ejemplo si es o no parte de la lista de dispositivos no autorizados, sus capacidades de seguridad y modo de unión (seguro o no seguro). Además el proceso de autentificación es diferente dependiendo del modo de operación del dispositivo central de seguridad (alta o estándar). En caso que el dispositivo nuevo sea rechazado por el dispositivo central de seguridad éste generará un mensaje para destitución del dispositivo y lo enviará al padre del mismo. El padre al recibirlo ordenará al nuevo dispositivo que salga de la red.

III.4 Conclusiones

Como puede observarse ZigBee no es un protocolo sencillo es su diseño, debido a que ha sido creado para dar solución a una gran variedad de aplicaciones cuyos requerimientos pueden ir desde lo más sencillo, como es el caso de la automatización del hogar, hasta alarmas de uso crítico para proteger la vida de los humanos. Por esta razón se ha buscado que el protocolo sea robusto, completo y seguro para lo cual se han implementado los elementos de seguridad

mencionados en secciones anteriores, y se realizan pruebas constantes de interoperabilidad del protocolo que además permiten realizar correcciones en el diseño del mismo. Además se creó un marco de trabajo que facilita el desarrollo de aplicaciones y la reutilización de comandos necesarios para diferentes tipos de dispositivos. Aún así, ZigBee es todavía un protocolo en desarrollo, enfocado principalmente a la interoperabilidad de dispositivos de diferentes marcas. En segundo término se buscó generar un perfil de aplicaciones para automatización del hogar. Por lo tanto el desempeño del protocolo en condiciones de estrés no ha sido oficialmente probado.

Sin embargo, la necesidad de facilitar el ingreso de ZigBee en ambientes cuyos requerimientos sean más estrictos, ha llevado al diseño de nuevas funcionalidades en el la revisión 2007 del protocolo. El estudio de ésta revisión queda fuera del alcance de ésta investigación, ya que no existe una versión disponible con la cual realizar pruebas de éstas nuevas funcionalidades y además la especificación se encontraba aún en desarrollo durante la realización de las pruebas de esta investigación.

CAPÍTULO IV

PRUEBAS PARA VERIFICACIÓN DE LAS CARACTERÍSTICAS DE ZIGBEE.

En este capítulo se explica el diseño e implementación de las pruebas realizadas al estándar ZigBee implementado en una versión de prueba de BeeKit liberada en Marzo del 2007 por la compañía Freescale. BeeKit[4] es una aplicación independiente que provee una interfaz gráfica de usuario en la cual se pueden crear, guardar y actualizar soluciones basadas en Simple MAC (SMAC) de Freescale, IEEE802.15.4 PHY/MAC y BeeStack ZigBee protocol stack. BeeKit provee un creador automático y explorador de soluciones que permite ajustar varios parámetros de la aplicación antes de crear el proyecto. La versión de prueba utilizada ha sido modificada repetidas veces durante los últimos 9 meses, por lo que algunos de los comportamientos podrían haber cambiando durante la realización de las pruebas que se presentan a continuación.

La finalidad principal de estas pruebas es observar el comportamiento del protocolo en aplicaciones con características similares a las ofrecidas por las redes cableadas de sensores, que actualmente satisfacen necesidades reales de los diferentes tipos de aplicaciones industriales que existen. En algunos casos estas

[4] http://www.freescale.com/

pruebas nos permiten verificar un comportamiento ya establecido por el estándar, para observar sus consecuencias en el desarrollo de la aplicación. En otros casos, la finalidad principal es encontrar un valor cuantitativo de alguna característica. Esto se debe a que algunos de los parámetros de comparación no han sido definidos aún por ZigBee Alliance. Debemos recordar que el nicho de aplicación inicial y prioritario considerado por la alianza ha sido el de las aplicaciones residenciales, por lo tanto no se ha realizado tanto énfasis en pruebas de estrés del protocolo, sino que las pruebas se han enfocado en la compatibilidad de los diferentes fabricantes, que por ahora es el problema más importante para ZigBee.

IV.1 Características Principales en el Análisis de Redes de Sensores.

Cómo se mencionó en capítulos anteriores, todas las redes de comunicación entre dispositivos cuentan con un conjunto de características comunes, que son las más importantes y necesarias para su estudio. En el Capítulo II se mencionó cuales eran estas características. Para poder comprender y comparar el estándar ZigBee con las necesidades de las aplicaciones inalámbricas de control o monitoreo industrial, es necesario conocer ésta lista de características.

Algunas de las características mencionadas en el Capítulo II son parte del estándar diseñado por la alianza, y se encuentran definidas en la especificación. Sin embargo, se realizarán pruebas para observar el funcionamiento del protocolo

poniendo en sus límites máximos y mínimos éstas características, con la finalidad de obtener una idea general de la manera en que la variación de estos parámetros afecta el desempeño de la red.

En cuanto a aquellas características que no son parte de la definición del protocolo, se les ha clasificado en dos tipos, aquellas que son fundamentales para comprender y calificar el comportamiento del protocolo ZigBee, y aquellas cuyo estudio, fuera de darnos información sobre el desempeño del protocolo en las aplicaciones de interés, nos desviarían del tema central de investigación. En el caso de las primeras se ha buscado que las pruebas diseñadas permitan obtener los valores de estas características para los que la red funciona apropiadamente. Para las del segundo grupo, se informará simplemente sobre los resultados obtenidos en otras investigaciones, si es que existen o bien se realizará un análisis sobre su relación con las necesidades de las aplicaciones industriales de monitoreo y control.

A continuación se mencionan las características del protocolo que serán probadas, las primeras cinco se encuentran definidas por el estándar, sin embargo a través de las pruebas diseñadas deseamos observar la reacción de la red ZigBee al cambiar los valores de éstas características. Las últimas tres características de ésta lista no se encuentran definidas por el estándar como un requerimiento para su implementación, y por lo tanto las pruebas realizadas buscan encontrar sus valores promedio y efectos en el desempeño de la red.

- Distancia
- Ancho de Banda.
- Numero de Dispositivos.
- Tamaño de mensajes.
- Redundancia.
- Respuesta en tiempo y variación.
- Integridad de datos.
- Eficiencia.

En la siguiente lista se mencionan las características del protocolo que serán analizadas por su definición en el protocolo o resultados de trabajos anteriores:

- Seguridad.
- Método de acceso.
- Topología.
- Soporte.
- Consumo de potencia.
- Capacidades.

Debido a que algunas de las pruebas permiten observar el efecto de varias características en el desempeño de la red, en la parte final de la definición de la prueba se realizará un listado de las características probadas y los resultados esperados.

IV.2 Formato de pruebas.

Para el formato de estas pruebas se utilizó como plantilla el formato de pruebas de interoperabilidad de Zigbee Alliance con algunos cambios, debido a que se le considera un formato sencillo y adaptable a las necesidades de la investigación realizada. El formato utilizado comprende los siguientes elementos:

- Título
- Descripción general.
- Condiciones iniciales
- Topología lógica
- Procedimiento.
- Salida.
- Características relacionadas con la prueba.

Al igual que las pruebas de interoperabilidad de Zigbee Alliance, las pruebas aquí presentadas toman como punto central una sola característica para cada tipo de prueba variando las condiciones bajo las que se puede evaluar. Por esta razón algunas de las pruebas resultan muy parecidas, sin embargo el punto focal es diferente en cada una.

IV.3 Aplicación de Pruebas.

Para realizar las pruebas fue necesario crear una aplicación que permitiera controlar el número y tamaño de los paquetes enviados, así como verificar la cantidad de paquetes que realmente fueron enviados o recibidos. La realización de esta aplicación resultó debido al marco de trabajo para aplicaciones (AF, Application Framework) del protocolo ZigBee. El marco de trabajo como se mencionó en el Capítulo III, consta del perfil de aplicación y la biblioteca de clusters. En general se utilizaron algunos de los comandos para pruebas de compatibilidad correspondientes a la aplicación del perfil de pruebas. En esta sección, se detallan los comandos tomados del perfil de pruebas de interoperabilidad de ZigBee, posteriormente se explica la realización de los comandos que fueron programados ya que su funcionalidad no estaba disponible dentro del perfil de pruebas. Finalmente, debido a la necesidad de verificar el número de paquetes enviados y recibidos por cada una de las capas del protocolo, fue necesario crear funciones y comandos especiales para resolver este problema. Su implementación se explica también en esta sección.

IV.4 Perfil de pruebas 2 (TP2, Test Profile 2)

Esta aplicación fue diseñada como una plataforma de comandos base para la realización de pruebas de interoperabilidad de la versión 1 de ZigBee para Automatización del Hogar. Dentro de este perfil de pruebas se describen una serie

de *clusters* utilizados para las pruebas de interoperabilidad. De tal lista únicamente se utilizan 3 *clusters* para las pruebas:

IV.4.1 Clusters Estandar

Esta sección se refiere a los clusters utilizados que forman parte del estándar ZigBee Test Profile 2.

Transmit Counted Packets (Identificador de cluster: 0x0001). Este cluster otorga la capacidad de enviar una cantidad determinada de mensajes de tamaño fijo y con un intervalo de tiempo dado entre ellos. Además al ser activado como cliente debe ser capaz de contar el número de mensajes de éste tipo que fueron recibidos.

Retrieve Counted Packets Request (Identificador de cluster 0x0003): Permite requerir a otro dispositivo el valor de su contador de Transmit Counted Packets, de ésta manera es posible saber el número de mensajes que fueron recibidos por la aplicación.

Retrieve Counted Packets Response (Identificador de Cluster: 0x0004): En respuesta al cluster anterior permite obtener el valor del contador de Transmit Counted Packets.

IV.4.2 Clusters Programados.

Además de los clusters tomados del TP2, fue necesario incluir algunos comandos para conteo de paquetes recibidos y enviados, por lo que se agregaron los siguientes cluster a la aplicación:

Transmit Request (Identificador de Cluster: 0x0005): A través de este cluster es posible inicializar el envío de Transmit Counted Packets, especificando el tamaño y número de los mensajes que serán transmitidos por el nodo receptor de este comando.

Packet Confirm Count Request (Identificador de Cluster: 0x0011): Permite requerir a un dispositivo el valor del contador de confirmaciones de los paquetes enviados.

Packet Confirm Count Response. (Identificador de Cluster: 0x0012): En respuesta al cluster anterior (0x0011), permite enviar a quien lo solicitó el valor del contador de paquetes enviados. La respuesta contendrá el conteo de paquetes que fueron detectados en los SAPs indicados en la Figura 7.

IV.5 Cliente de Pruebas ZigBee

Una de las cualidades más importantes del protocolo ZigBee son los puntos de acceso a servicios (SAPs, Service Access Points) localizados entre las capas. Su importancia radica en la posibilidad de que una aplicación pueda conectarse a

éstos puntos de acceso y enviar, recibir o monitorear mensajes hacia las capas. En la versión de prueba del protocolo ZigBee que fue utilizada existe tal aplicación y se le llama Cliente de Pruebas ZigBee (ZTC, ZigBee Test Client).

Ésta aplicación fue utilizada para monitorear el número de paquetes que eran enviados a través de los puntos de acceso correspondientes a las capas APS, NWK y de aplicación. Ya sea que correspondieran a un mensaje generado por la aplicación y enviado por el aire hacia otro dispositivo o bien en el caso de indicaciones de mensajes que llegaron a través del radio son transferidos por todas las capas hasta la aplicación.

A continuación en la Tabla VII se mencionan los comandos monitoreados en cada uno de los puntos de acceso:

Tabla VII. Comandos interceptados por la aplicación del ZTC en los SAPs del protocolo

Tipo de Comando		Punto de Acceso de Servicios
Envío de paquete de datos	Data Request	APSDE-SAP
Envío de paquete de datos	Data Request	NLDE-SAP
Confirmación de envío de paquete de datos	Data request confirm	NLDE-SAP
Confirmación de envío de paquete de datos	Data request confirm	APSDE-SAP
Confirmación de envío de paquete de datos	Data request confirm	MAC
Indicación de recepción de un paquete de datos	Data Indication	NLDE-SAP

Indicación de recepción de un paquete de datos	Data Indication	APSDE-SAP
Indicación de recepción de un paquete de datos	Data Indication	MAC

En la Figura 7 se muestra la localización de los puntos de acceso en la arquitectura del protocolo ZigBee, y se muestra el ZTC como una aplicación externa que se conecta a estos puntos para monitorear el tipo y cantidad de mensajes que pasan por ellos.

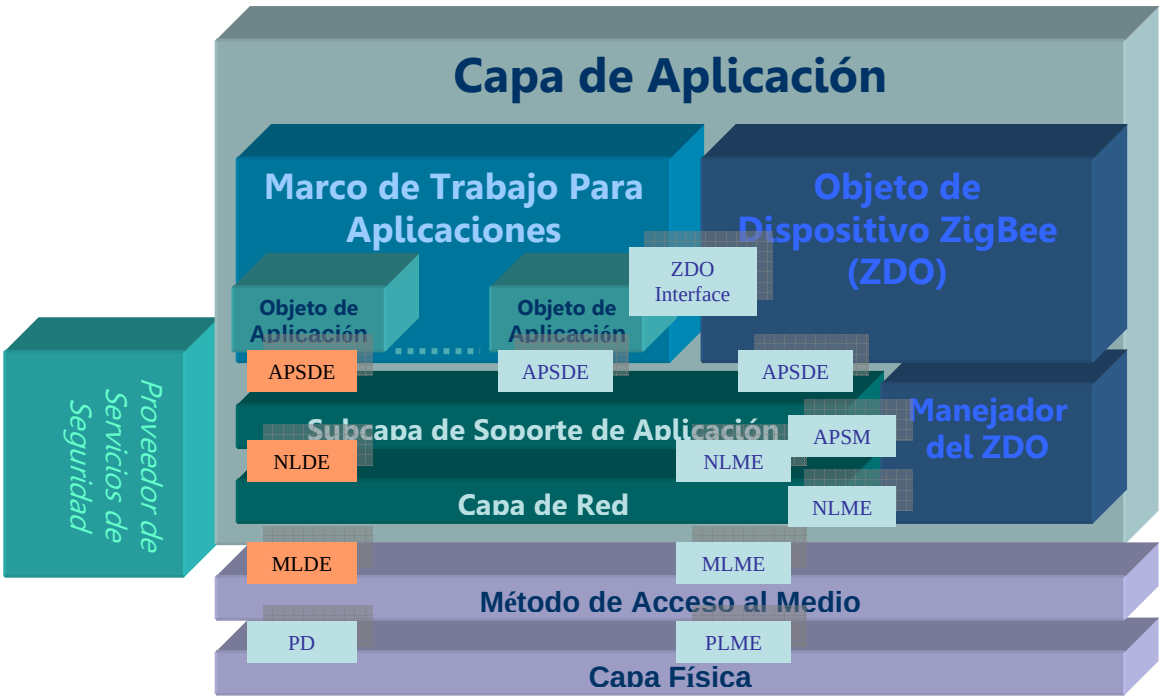


Figura 7. Inyección e Intercepción de Paquetes con ZTC

Debido a que el número de paquetes contados no se refiere únicamente a aquellos que llegan a la aplicación, sino también a aquellos que son transferidos entre las capas de NWK y APS, el cluster Retrieve Counted Packets Response, fue modificado para poder responder con la cuenta de todos estos valores en lugar de responder únicamente con los dos bytes correspondientes a la cuenta de paquetes en la aplicación.

La razón que justifica contar los paquetes transferidos a través de los puntos de acceso y no solamente aquellos que llegan a la capa de aplicación, es verificar la capa en que se pierde la mayor cantidad de paquetes recibidos o transmitidos.

IV.6 Sensor Network Analyzer (SNA)

Una de las herramientas más utilizadas para la realización de las pruebas, en esta investigación, es el analizador de redes de sensores de la compañía Daintree[5]. Este dispositivo consiste en un pequeño receptor que puede ser ajustado a la frecuencia del canal en que una red IEEE 802.15.4 está trabajando. Y con un software como el que se muestra en la Figura 8, diseñado para dar formato a los mensajes que el receptor percibe en el canal, puede desplegar la información del mensaje en diferentes formas para un mejor análisis por parte del usuario.

[5] http://www.daintree.net/

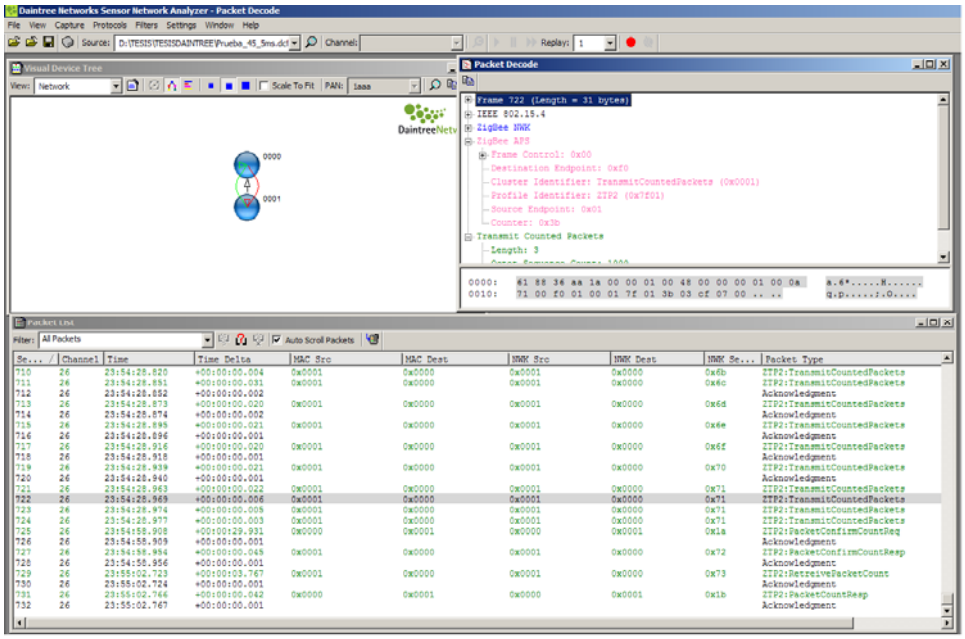


Figura 8. Muestra de una captura tomada por el SNA de la compañía Diantree

El analizador de redes de sensores de esta compañía es también el más utilizado para las pruebas de interoperabilidad de ZigBee. Utilizando este analizador de redes resulta mucho más sencillo capturar el envío de mensajes a través del canal de frecuencia seleccionado, lo que facilita la observación de los resultados de las pruebas.

IV.7 Descripción de Pruebas

Esta sección se encuentra dedicada a la descripción del diseño de las pruebas y su implementación, los resultados obtenidos se analizan posteriormente en el Capítulo V. Como se mencionó anteriormente, el formato está basado en el

utilizado para las pruebas de interoperabilidad ZigBee, pero se realizaron algunos cambios para adaptarlo a las pruebas que se realiza. Por ejemplo, debido a que no existe una salida exitosa o de fallo, esa parte del formato fue removida y en su lugar se agregó la lista de características de la red con que puede ser relacionada la prueba.

IV.8 Ambientes de Prueba

Aún cuando el ambiente de los entornos industriales resulta particularmente diferente al de cualquier entorno utilizado para las pruebas de este trabajo, no sería posible definir un ambiente específico para realizarlas, sin delimitar los resultados al tipo de aplicaciones que se den en ese tipo de ambiente. Por esta razón más allá que enfocarnos en ambientes específicos de prueba, se decidió utilizar ambientes sencillos y enfocar las conclusiones en base a las características comprobables del protocolo.

Los ambientes utilizados para la realización de las pruebas son los siguientes:

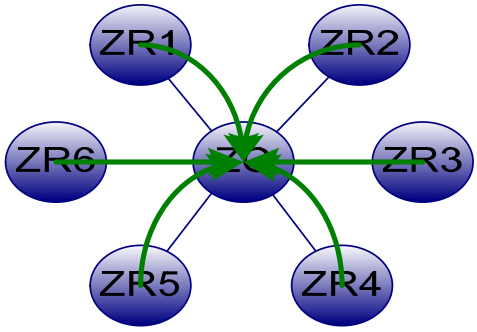
- Exterior al aire libre: área de estacionamiento de CICESE en horarios en que se encuentra vacío.
- Interiores:
- Para mediciones de distancia se utilizó el pasillo lateral del tercer piso del edificio de la División de Física Aplicada del CICESE.
- Dimensiones: 2 x 21 metros cuadrados

- Otras características: espacio cerrado sin ventanas y con puertas de madera cerradas, cuenta con red inalámbrica y se encontraron redes Bluetooth en las cercanías.
- Para mediciones cercanas se utilizó el área de trabajo de la empresa Ubilogix.
- Dimensiones: 6 m ancho por 15 de largo, el área utilizada es una mesa de madera de 1.7 m de largo por 90 cm de ancho.
- Otras características: El espacio se encuentra cerrado, cuenta con mesas, computadoras y red inalámbrica.

Prueba 1. Integridad de los datos - Estrella

Descripción general. Durante esta prueba se mide el efecto que tiene el aumento de nodos en la red sobre la integridad de los datos. Durante esta prueba se cambiarán dos parámetros importantes, el tamaño de la red y la velocidad de envío de los paquetes. La prueba que se describe a continuación deberá realizarse con diferentes periodos de envío de paquetes: 5, 10 y 20 milisegundos, son los tiempos que pueden obtenerse en redes alambradas de sensores que se utilizan actualmente, por lo tanto las pruebas se realizaron inicialmente con éstas velocidades. Sin embargo, debido a los resultados observados se decidió aumentar el tiempo a 40 y 50 milisegundos. La razón de este cambio en el diseño de la prueba se explica con mayor detalle en el Capítulo V, correspondiente al análisis de resultados.

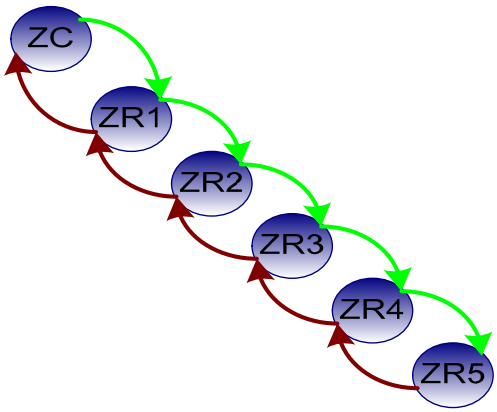
Tabla VIII. Descripción de la Prueba 1 Integridad de los datos – Estrella

<table>
<tr><td colspan="3">TOPOLOGÍA LÓGICA</td></tr>
<tr><td colspan="2"> 
</td><td></td></tr>
<tr><td colspan="3">CONDICIONES INICIALES</td></tr>
<tr><td>1</td><td colspan="2">ZC Forma la red con PanID 0x1AAA</td></tr>
<tr><td>2</td><td colspan="2">ZRs están programados con los comandos mencionados para transmisión de mensajes hacia el ZC</td></tr>
<tr><td>3</td><td colspan="2">Periodo de transmisión: 5, 10, 20, 40 y 50 milisegundos
Tamaño de mensaje: Mínimo = 1 byte Máximo = 80 bytes
Tamaño máximo de la red = 7 nodos</td></tr>
<tr><td colspan="3">PROCEDIMIENTO</td></tr>
<tr><td>Paso</td><td>Descripción</td><td>Salida</td></tr>
<tr><td>1</td><td>Agregue un nodo a la red y comience el envío de 1000 mensajes utilizando el comando Transmit Request con los datos especificados en las condiciones iniciales.</td><td>1</td></tr>
<tr><td>2</td><td>Verifique la cantidad de paquetes enviados y recibidos utilizando los comandos Retrieve Counted Packets request y Packet Confirm Count request.</td><td></td></tr>
<tr><td>3</td><td>Repita los pasos anteriores hasta obtener el tamaño máximo de la red.</td><td></td></tr>
<tr><td colspan="3">SALIDA</td></tr>
<tr><td>1</td><td colspan="2">Verifique la cantidad total de mensajes recibidos y transmitidos.</td></tr>
<tr><td colspan="3">CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA</td></tr>
<tr><td colspan="3">Integridad de los datos conforme cambian las siguientes características:
Ancho de banda disponible para cada dispositivo.
Tamaño de la red.
Tamaño del mensaje.
Periodo de transmisión.</td></tr>
</table>

Prueba 2. Integridad de los datos - Multisalto

Descripción general. Esta prueba pretende medir el efecto sobre la integridad de la red que tiene el aumento en el número de saltos que puede dar un mensaje en una red de tipo árbol. Al igual que en la Prueba 1, se cambian dos parámetros importantes: el tamaño de la red y la velocidad de envío de los paquetes.

Tabla IX. Descripción de la Prueba 2 Integridad de los datos - Multisalto

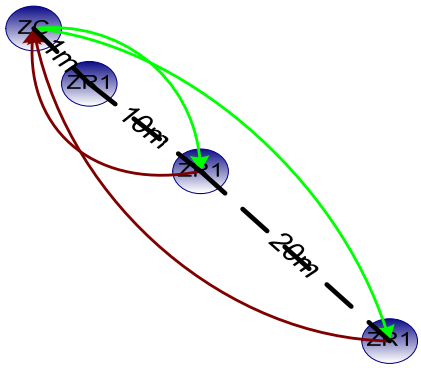
TOPOLOGÍA LÓGICA	
	
CONDICIONES INICIALES	
1	ZC Forma la red con PanID 0x1AAA
2	ZRs están programados con los comandos mencionados para transmisión de mensajes hacia el ZC
3	Periodo de transmisión: 5, 10, 20, 40 y 50 milisegundos Número máximo de saltos = 5 Tamaño de mensaje: Mínimo = 1 byte Máximo = 80 bytes
4	Para verificar el envío y recepción de los datos debe utilizarse un analizador de red inalámbrica o bien generar una acción en el ZC para el conteo de los mensajes recibidos.

PROCEDIMIENTO		
Paso	Descripción	Salida
1	Una un ZR al ZC y comience el envío de mensajes utilizando el comando Transmit Request desde el ZC	1
2	Una el ZRx+1 al ZRx (x=0:4) comience el envío de mensajes desde el ZRx+1 hacia el ZC utilizando el Transmit Request	
3	Repita hasta que X+1= máximo número de saltos	
SALIDA		
1	Verifique la cantidad total de mensajes recibidos y transmitidos	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Integridad de los datos conforme cambian las siguientes características: Número de saltos. Tamaño del mensaje. Periodo de transmisión.		

Prueba 3. Integridad de los datos - Distancia

Descripción general. Envío y recepción de 1000 mensajes a diferentes distancias para verificar la cantidad de paquetes perdidos y la posibilidad de conexión de acuerdo al aumento de distancia entre los nodos.

Tabla X. Descripción de la Prueba 3 Integridad de los datos - Distancia

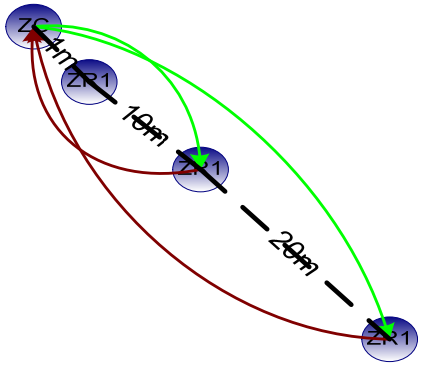
TOPOLOGÍA LÓGICA	
	
CONDICIONES INICIALES	
1	ZC Forma la red con PanID 0x1AAA
2	El ZR está programado para responder los comandos Transmit Request y Retrieve Counted Packets, así como para generar Transmit Counted Packets y Packet Count Request
3	Para verificar el envío y recepción de los datos debe utilizarse un analizador de red inalámbrica o bien generar una acción en el ZC para el conteo de los mensajes recibidos.
4	Tiempo de muestreo: 5, 10, 20, 40 y 50 milisegundos Tamaño de mensaje: Mínimo = 1 byte Máximo = 104 bytes Distancia Máxima = 75 m
5	Ambientes: Interior. Pasillo del tercer piso del edificio de la División de Física Aplicada en CICESE, puertas laterales cerradas y con línea de vista entre los nodos. Exterior. Estacionamiento del edificio de Oceanología, línea de vista entre los

	nodos.	
PROCEDIMIENTO		
Paso	Descripción	Salida
1	Midiendo una distancia de 1m entre el ZC y el ZR1 inicie el envío de mensajes utilizando Transmit Request desde el ZC.	1
2	Aumente la distancia en 1m y repita el envío de los mensajes. Al llegar a 10 m las siguientes distancias medidas serán múltiplos de 10. (Ejemplo: 10 m, 20 m...100 m).	
3	Repita el paso 2 hasta llegar a la distancia máxima o hasta que la conexión entre los nodos no sea posible.	
4	Realice la prueba en ambos ambientes, interior y exterior.	
SALIDA		
1	Número total de mensajes recibidos	
2	Distancia máxima en que la conexión entre los nodos es posible	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Se verifica como afecta la integridad de los datos de acuerdo a las variaciones en: Distancia. Tamaño de mensajes. Ambiente. Periodo de transmisión.		

Prueba 4. Tiempo de respuesta – Distancia

Descripción general. Envío y recepción de varios mensajes a diferentes distancias para verificar latencia.

Tabla XI. Descripción de la Prueba 4 Tiempo de respuesta – Distancia

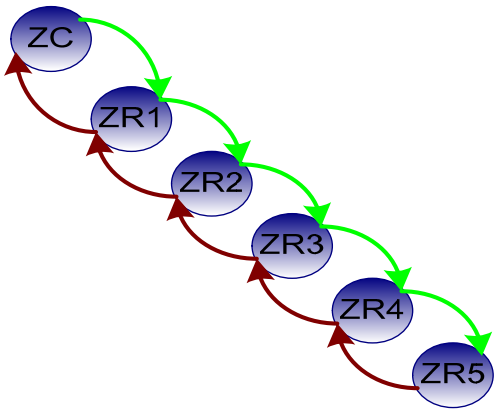
TOPOLOGÍA LÓGICA		
		
CONDICIONES INICIALES		
1	ZC Forma la red con PanID 0x1AAA	
2	El ZR está programado para responder los comandos Transmit Request y Retrieve Counted Packets, así como para generar Transmit Counted Packets y Packet Count Request	
3	Para verificar el envío y recepción de los datos debe utilizarse un analizador de red inalámbrica o bien generar una acción en el ZC para el conteo de los mensajes recibidos.	
4	Distancia Máxima = 75 m	
PROCEDIMIENTO		
Paso	Descripción	Salida
1	Midiendo una distancia de 1 m entre el ZC y el ZR1 realice la petición de 1 Transmit Counted Packet utilizando el comando Transmit Request	1
2	Aumente la distancia en 1m y repita el envío de los mensajes. Al llegar a 10 m las siguientes distancias medidas serán múltiplos de 10. (Ejemplo:	

	10 m, 20 m...100 m).	
3	Repita el paso 2 hasta llegar a la distancia máxima o hasta que la conexión entre los nodos no sea posible.	
4	Realice la prueba en ambos ambientes, interior y exterior.	
SALIDA		
1	Verifique la diferencia de tiempo, en el analizador de red, entre el comando Transmit Request y el Transmit Counted Packet.	
2	Distancia máxima en que la conexión entre los nodos es posible	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Se verifica como afecta al tiempo de respuesta las variaciones en la distancia.		

Prueba 5. Tiempo de respuesta – Multisalto.

Descripción general. Esta prueba permite medir el tiempo de retraso que causan los saltos necesitados para que un mensaje llegue a su destino. Este tipo de situación será muy común en una red de topología árbol, o bien en una red en que los nodos se encuentren muy alejados y deban hacer uso de las capacidades de enrutamiento de la red.

Tabla XII. Descripción de la Prueba 5 Tiempo de respuesta - Multisalto

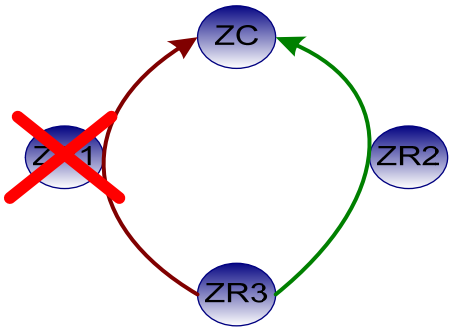
TOPOLOGÍA LÓGICA	
	
CONDICIONES INICIALES	
1	ZC Forma la red con PanID 0x1AAA
2	El ZR está programado para responder los comandos Transmit Request y Retrieve Counted Packets, así como para generar Transmit Counted Packets y Packet Count Request
3	Para verificar el envío y recepción de los datos debe utilizarse un analizador de red inalámbrica o bien generar una acción en el ZC para el conteo de los mensajes recibidos.
4	Número máximo de saltos: 5. Distancia máxima = 75 m.

PROCEDIMIENTO		
Paso	Descripción	Salida
1	Una un ZR al ZC y realice la petición de un mensaje Transmit Counted Packet haciendo uso del comando Transmit Request.	1
2	Una el ZRx+1 al ZRx (x=0:4) y repita la petición del mensaje desde el ZRx+1 hacia el ZC utilizando el Transmit Request	
3	Repita hasta que X+1= máximo número de saltos	
SALIDA		
1	Verifique la diferencia de tiempo, en el analizador de red, entre el comando Transmit Request y el Transmit Counted Packet.	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Se verifica como afecta al tiempo de respuesta la cantidad de saltos que se necesitan para que el mensaje llegue a su destino.		

Prueba 6. Tiempo de recuperación de ruta - Redundancia.

Descripción general. Verifica el tiempo que tarda un dispositivo en encontrar una ruta alterna para un mensaje, al detectar que la ruta utilizada previamente ya no se encuentra disponible.

Tabla XIII. Descripción de la Prueba 6 Tiempo de recuperación de ruta - Redundancia

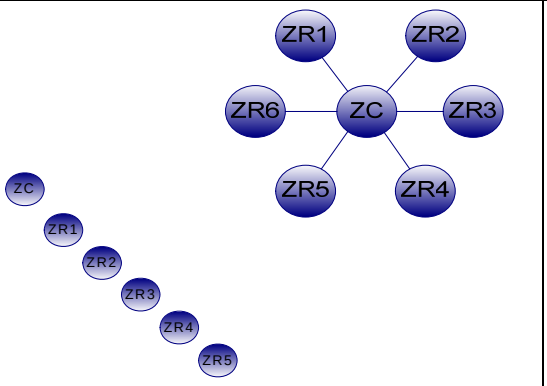
TOPOLOGÍA LÓGICA		
		
CONDICIONES INICIALES		
1	ZC Forma la red con PanID 0x1AAA	
2	El ZR está programado para responder los comandos Transmit Request y Retrieve Counted Packets, así como para generar Transmit Counted Packets y Packet Count Request	
3	Para verificar el envío y recepción de los datos debe utilizarse un analizador de red inalámbrica o bien generar una acción en el ZC para el conteo de los mensajes recibidos.	
4	Número máximo de saltos: 5. Distancia máxima = 75m.	
PROCEDIMIENTO		
Paso	Descripción	Salida

1	Utilizando el comando Transmit Request ordene al ZR3 que comience el envío de mensajes Transmit Counted Packets.	1
2	Antes de que la transmisión de mensajes del ZR3 al ZC haya terminado, apague el ZR por el que estos mensajes están siendo transferidos al coordinador (ZR1 o ZR2)	2
3	Verifique el tiempo que tarde el ZR3 en encontrar la nueva ruta a través del ZR que aún se encuentra encendido.	
SALIDA		
1	Verifique que el ZR3 haya encontrado una nueva ruta y haya continuado el envío de mensajes	
2	Verifique la diferencia en tiempo en el analizador de red, entre el envío del último mensaje por la ruta inicial y el envío del primer mensaje por la nueva ruta encontrada.	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Esta prueba permite medir el tiempo que tarda un nodo enrutador en encontrar una nueva ruta cuando la que está utilizando falla. También se observa la influencia del periodo de transmisión de los mensajes en el tiempo de búsqueda de la nueva ruta.		

Prueba 7. Tiempo de Conexión

Descripción general. Permite verificar el tiempo que toma la unión de un dispositivo a una red con cualquiera de las configuraciones básicas: estrella o en árbol.

Tabla XIV. Descripción de la Prueba 7 Tiempo de conexión

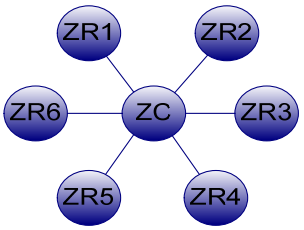
TOPOLOGÍA LÓGICA		
		
CONDICIONES INICIALES		
1	Para la configuración estrella se utilizarán tanto ZRs como ZEDs	
PROCEDIMIENTO		
Paso	Descripción	Salida
1	Agregue uno a uno 6 ZR al coordinador en topología estrella y verifique el tiempo que toma en conectarse cada uno.	1
2	Agregue uno a uno 5 ZR al coordinador en topología árbol y verifique el tiempo que toma en conectarse cada uno.	2
3	Agregue uno a uno 14 ED al coordinador y verifique el tiempo que toma en conectarse cada uno.	
SALIDA		

1	Tiempo de conexión de ZR en configuración estrella.
2	Tiempo de conexión de ZR en configuración árbol.
3	Tiempo de conexión de ZED en configuración estrella.
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA	
Esta prueba permite observar los efectos en el tiempo de creación de una red, variando dos parámetros: Tipo de topología creada. Tipo de dispositivos utilizados.	

Prueba 8. Conexiones simultaneas

Descripción general. Permite verificar la cantidad máxima de nodos que puede unirse a un dispositivo al mismo tiempo.

Tabla XV. Descripción de la Prueba 8 Conexiones simultáneas

TOPOLOGÍA LÓGICA		
		
CONDICIONES INICIALES		
1	Para simular la unión simultánea es necesario que sea posible encender los nodos al mismo tiempo, para lo cual se recomienda utilizar una fuente con multiples conexiones y un solo interruptor.	
PROCEDIMIENTO		
Paso	Descripción	Salida
1	Encienda los x routers al mismo tiempo para que inicien el proceso de conexión	1
2	Actualice el valor de x=x+1 y repita el paso 1	
3	Verifique cual es la cantidad de dispositivos que pudieron unirse a la red del ZC	
SALIDA		
1	Cantidad máxima de nodos unidos simultáneamente.	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Esta prueba permite verificar que tan grande puede ser un conjunto de nodos que sea energizado simultáneamente para que la red pueda ser formada.		

Prueba 9. Tamaño de la red – Capacidad máxima

Descripción general. Verifica que se puedan unir al menos 32 nodos a la red. Debido a que el mínimo número de nodos que ofrece una red cableada es de 32, esta prueba permite verificar la posibilidad de unir al menos esta misma cantidad de nodos inalámbricos.

Tabla XVI. Descripción de la Prueba 9 Tamaño de la red – Capacidad máxima

TOPOLOGÍA LÓGICA		
		
CONDICIONES INICIALES		
1	ZC Forma la red con PanID 0x1AAA.	
2	Todos los nodos de la red unidos posteriormente son ZR y se verifica la recepción de mensajes a través del encendido de un LED	
3	Realice dos pruebas tipos de pruebas para los dos enrutamientos posibles: malla y árbol.	
PROCEDIMIENTO		
Paso	Descripción	Salida
1	Agregue uno a uno los ZR a la red y verifique el tiempo total que toma conectarlos.	

2	Repita el procedimiento utilizando ZED hasta llenar cada nivel de profundidad. Verifique el tiempo total de conexión de la red	
3	Envíe al menos 20 comandos broadcast y verifique su expansión a través de toda la red.	1
4	Envíe un mensaje Transmit Request desde el ZC hasta un nodo fuera de la distancia de transmisión del mismo.	2
SALIDA		
1	Cantidad máxima de nodos que reciben la totalidad de los mensajes enviados.	
2	Verifique el tiempo de respuesta del nodo con la diferencia de tiempo entre el comando Transmit Request y la respuesta Transmit Counted Packet.	
CARACTERÍSTICAS RELACIONADAS CON LA PRUEBA		
Esta prueba permite verificar que los mensajes *broadcast* sean recibidos por todos los nodos que comprenden una red de tamaño 32. Además permite verificar el tiempo de respuesta en una red densa de tamaño 32.		

IV.9 Conclusiones

La realización de las pruebas mostró resultados interesantes que se analizan con mayor detalle en los dos capítulos posteriores. Cabe destacar que fue necesario modificar el formato de las pruebas debido a la necesidad de incluir información relacionada con las características específicas de las pruebas. Durante el proceso de las pruebas y de acuerdo a los resultados obtenidos fue necesario realizar cambios en algunos parámetros como el periodo de envío de los mensajes y la altura a la que se colocaron los nodos, esto con la finalidad de obtener resultados concluyentes sobre algunas de las características del protocolo.

Se puede considerar que la elección de las herramientas y pruebas realizadas, así como el diseño de las mismas fue el apropiado para obtener la información deseada acerca de las características del protocolo ZigBee que se están estudiando.

CAPÍTULO V

Análisis de Resultados

Para destacar finalmente las ventajas y desventajas de una red ZigBee utilizada en un ambiente industrial, en este capítulo se realiza una comparación de los resultados obtenidos en las pruebas definidas en el Capítulo IV y los valores encontrados en redes industriales de sensores cableadas en el Capítulo II.

V.1 Ancho de Banda

Como se mencionó en el Capítulo II, la ampliación del ancho de banda ha sido una de las mejoras más importantes que ofrecen varios protocolos para comunicación de redes de sensores cableadas, sobre todo a partir de la aparición de Industrial Ethernet. Sin embargo, la necesidad de mayor o menor ancho de banda es una característica que depende en gran medida de la aplicación en que se utilizará la red, por lo que pueden encontrarse redes sencillas, con anchos de banda pequeños y que son ampliamente utilizadas en aplicaciones que no requieren de un envío masivo de información. De acuerdo al estudio de redes cableadas realizado en el Capítulo II, en la Tabla XVII se muestran los anchos de banda que ofrecen algunos de los protocolos más importantes:

Tabla XVII. Anchos de banda de redes cableadas de sensores

Protocolo	Ancho de Banda
AS-i	49.6 kbps
CAN	125 kbps -1 Mbps
Foundation H1	500 kbps -31.25 kbps
Ethernet/IP	10/100/1000 Mbps

Al comparar los valores de la Tabla XVII (tomados de la investigación realizada en el Capítulo II) con el protocolo ZigBee que utiliza 16 canales de 2.4 GHz con un ancho de banda de 250 kbps, se puede ver que esta característica restringe el protocolo al tipo de aplicaciones en que se utilizan versiones antiguas de CAN o Foundation H1. Sin embargo, ZigBee tiene suficiente capacidad para ser utilizado en las aplicaciones del nivel jerárquico más bajo, como monitoreo y control de sensores y actuadores de campo. Es importante resaltar que los anchos de banda mencionados en la Tabla XVII son únicamente los establecidos por el estándar de capa física mencionado, pueden existir mecanismos en capas superiores de estos protocolos que disminuyan los valores mostrados.

Ahora bien, en la práctica lo que realmente importa en una aplicación es la capacidad de utilizar el ancho de banda que tengan los nodos. Por lo tanto, se realizaron pruebas para verificar la capacidad de los nodos ZigBee en recepción y transmisión de mensajes. Una de las pruebas más interesantes sobre esta característica es la Prueba 1 *Integridad de los datos - Estrella*. Durante esta prueba

se intentó enviar 1000 mensajes de 1 byte de carga útil con el formato del protocolo ZigBee para Transmit Counted Packets, en una red que varió de tamaño de 2 a 7 nodos, con un solo nodo como receptor y 1 a 6 nodos como transmisores de los mensajes.

En el caso de la prueba el mensaje enviado tiene un total de 29 bytes, 25 correspondientes a los encabezados de las capas MAC, NWK y APS y 4 bytes de carga útil debido al tipo de mensaje utilizado (Transmit Counted Packets). Por lo tanto, se esperaría que, con un ancho de banda de 250 kbps, un solo nodo con desempeño ideal fuese capaz de enviar 1 mensaje de este tamaño cada milisegundo, sin embargo, las hojas de datos de los nodos utilizados aseguran únicamente un mensaje de 128 bytes cada 4 ms. Por lo que los tiempos de 10, 20, 40 y 50 ms deberían ser suficientes para el envío de un paquete de este tamaño, suponiendo que la creación de cada paquete toma al menos 4 veces el tiempo de transmisión. Sin embargo, de acuerdo a los resultados mostrados en la Figura 9 el uso práctico del ancho de banda está restringido por la capacidad de procesamiento del nodo.

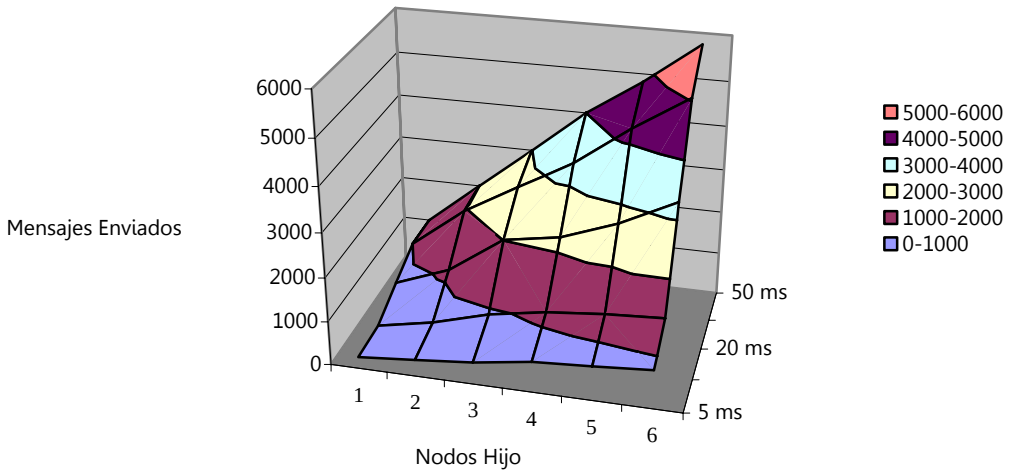


Figura 9. Resultados de la Prueba 1. Integridad de los datos – Estrella. Se muestra la cantidad de mensajes transmitidos para una mínima carga útil

A pesar de que el comando especifica el envío de mensajes cada 5 ms, la aplicación no es capaz de hacerlo. En lugar de eso un nodo sólo es capaz de transmitir la totalidad de los mensajes a partir de un periodo de 40 ms y hacia valores mayores. Puede observarse que solo para los periodos de 40 y 50 ms la gráfica tiene un comportamiento casi lineal al crecer el tamaño de la red. Sin embargo, se generan retrasos y pérdidas de paquetes debido a las colisiones y reintentos de envío por encontrarse el canal ocupado. Ahora bien, en la Figura 10 se muestran los resultados de la misma prueba para un tamaño de carga útil máximo de 80 bytes, permitido por ZigBee. Los mensajes tienen este tamaño debido a la restricción en el tamaño máximo de APSDU por depender del tamaño

de los encabezados de algunos comandos del ZDO. Sin embargo es posible modificar la aplicación para utilizar los 128 bytes de la trama.

Puede observarse que en el caso de los mensajes de mayor tamaño, se tiene un comportamiento cercano a la linealidad. Sin embargo se tiene una meseta debido a la cercanía de los valores para los casos de 3 y 4 nodos hijo en un periodo de 40 ms. Además sucede un fenómeno interesante en el caso de 5 ms entre estos mismos nodos, pues se observa que el valor total de mensajes enviados resulta menor para el caso de 4 nodos que para el de 3. Es posible que la razón de esto sea que con un mayor tamaño de mensaje, el canal se encuentra ocupado durante un lapso mayor de tiempo, provocando la pérdida de más mensajes de los nodos vecinos.

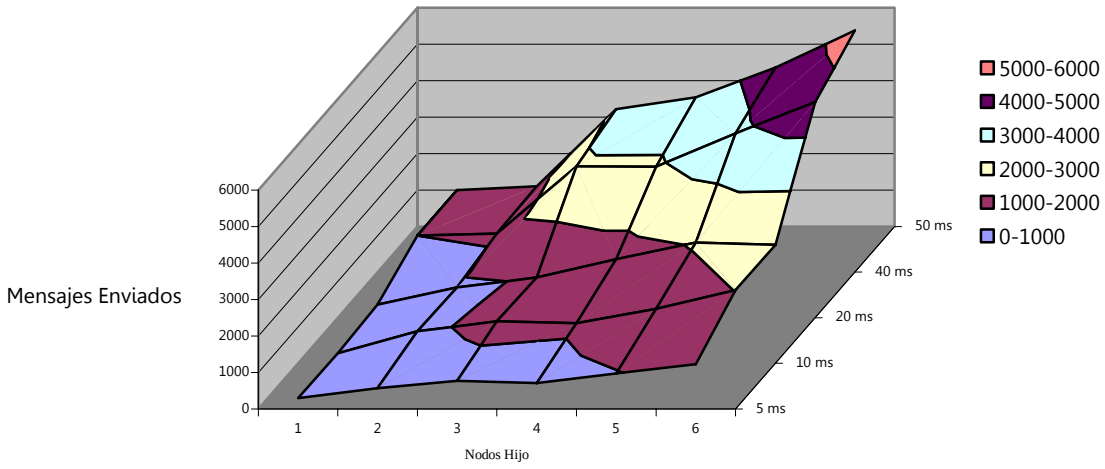


Figura 10. Resultados de la *Prueba 1. Integridad de los datos – Estrella*. Se muestra la cantidad de mensajes transmitidos para una máxima carga útil

Por último se muestra la Figura 11 en la cual puede observarse que a excepción del pequeño traslape entre la cantidad máxima (MAX) de bits transmitidos en mensajes con carga útil de tamaño mínimo (Mínima Carga Útil) y la cantidad mínima (MIN) de bits transmitidos en mensajes de carga útil de tamaño máximo (Máxima Carga Útil), la cantidad de bits enviados en el caso del tamaño máximo de mensaje es siempre mayor que en el caso de un tamaño mínimo de mensaje.

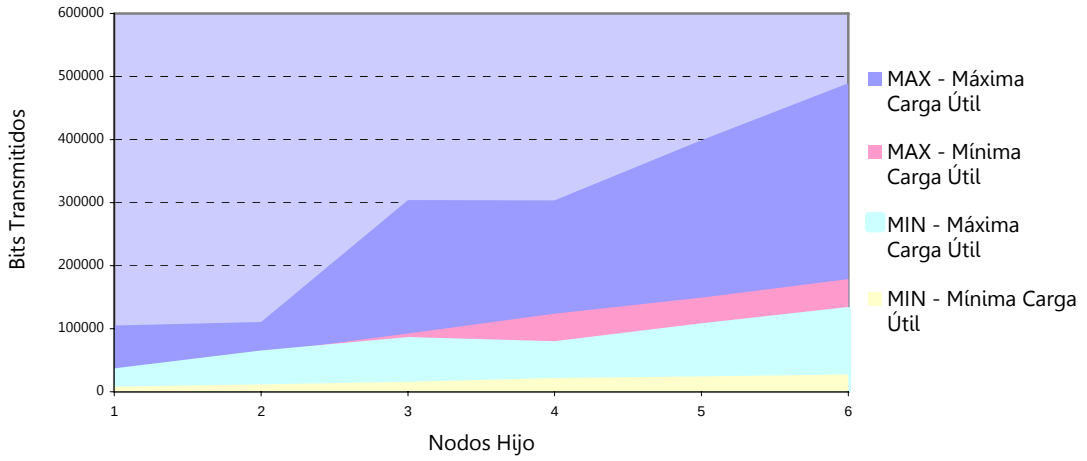


Figura 11. Comparación de los resultados de la *Prueba 1. Integridad de los datos – Estrella*. Se muestra las cantidades máximas (MAX) y mínimas (MIN) de bits transmitidos, enviando mensajes con los dos tamaños de carga útil definidos como Mínima Carga Útil y Máxima Carga Útil

Sin embargo en la Figura 12 se muestra que la cantidad máxima y mínima de mensajes enviados en la Prueba 1 *Integridad de los datos* - *Estrella* es muy parecida para los dos tamaños de mensajes utilizados, lo que nos permite corroborar que el retardo principal está en la generación de los encabezados de cada una de las capas, ya que sin importar la cantidad de bytes contenidos en la carga útil, la cantidad de mensajes enviados es muy similar.

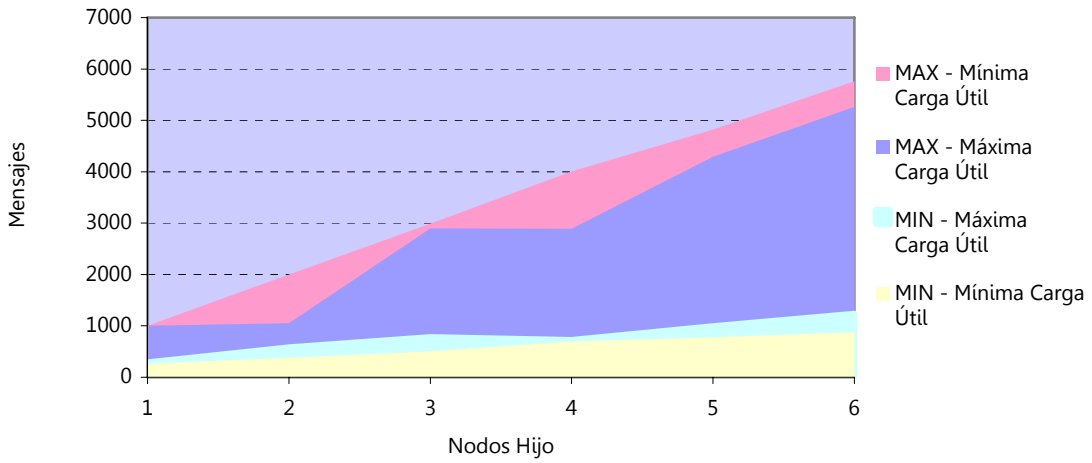


Figura 12. Comparación de los resultados de la *Prueba 1. Integridad de los datos – Estrella*. Se muestra las cantidades máximas (MAX) y mínimas (MIN) de mensajes transmitidos, enviando mensajes con los dos tamaños de carga útil definidos como Mínima Carga Útil y Máxima Carga Útil

Hasta ahora solo se han descrito los resultados en la transmisión de mensajes, sin embargo una parte aún más importante es la recepción; si el receptor

no es capaz de procesar todos los mensajes enviados, no tiene sentido enviar el máximo posible.

Para mostrar la capacidad de recepción y procesamiento de mensajes se deben comparar la Figura 13 y Figura 14. En la primera se observa la cantidad máxima y mínima de mensajes recibidos a medida que aumenta la cantidad de nodos en la red, tanto para un tamaño máximo de carga útil como para el tamaño mínimo. En cambio en la Figura 14 se observa la cantidad de bits recibidos (Nótese que el orden de las líneas ha sido modificado para que queden de mayor a menor valor en ambas figuras).

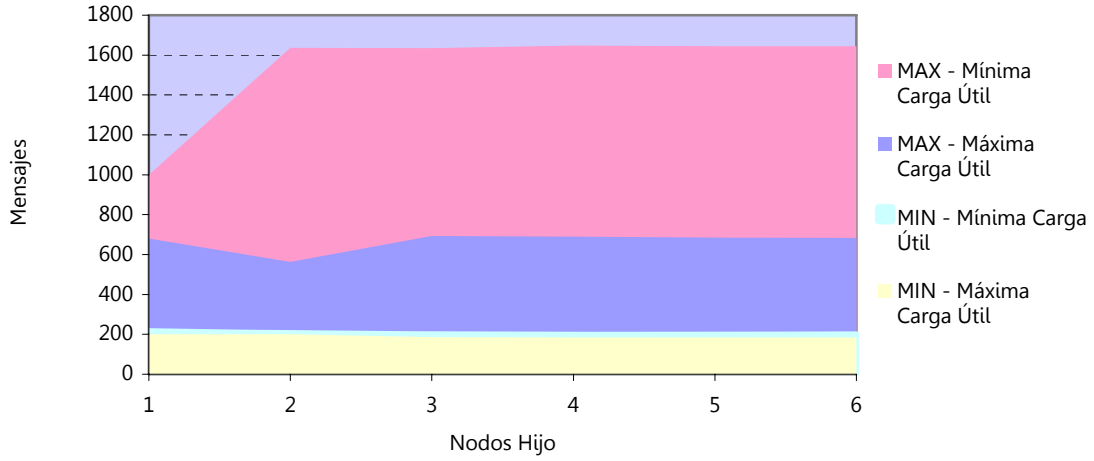


Figura 13. Comparación de los resultados de la *Prueba 1. Integridad de los datos – Estrella*. Se muestra las cantidades máximas (MAX) y mínimas (MIN) de mensajes recibidos, en mensajes con los dos tamaños de carga útil definidos como Mínima Carga Útil y Máxima Carga Útil

Al comparar estas dos gráficas, se puede notar de nuevo que a pesar de haber sido recibidos menos mensajes de mayor tamaño, la cantidad de bits de carga útil sigue siendo mayor. Puede concluirse que durante la recepción de los mensajes, el retiro de los encabezados necesita más procesamiento. Y además para el caso de los mensajes con carga útil de tamaño máximo, se hace notorio que el receptor no puede procesar más de 1600 mensajes aproximadamente, sin importar cuántos mensajes sean capaces de enviar los nodos transmisores.

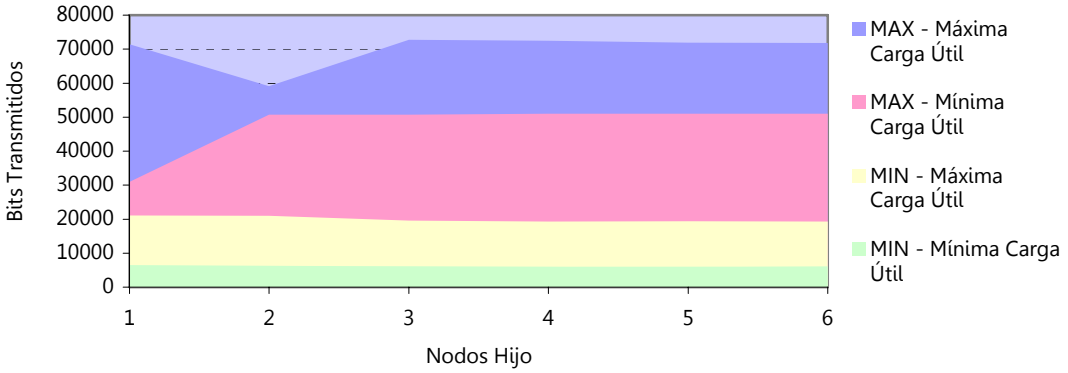


Figura 14. Comparación de los resultados de la *Prueba 1. Integridad de los datos – Estrella*. Se muestra las cantidades máximas (MAX) y mínimas (MIN) de bits recibidos, en mensajes con los dos tamaños de carga útil definidos como Mínima Carga Útil y Máxima Carga Útil

V.2 Eficiencia

Calculando la eficiencia como el porcentaje máximo de carga útil respecto al tamaño total del mensaje, esta sería de 81.2% para ZigBee, sin embargo, es más interesante analizar los resultados de eficiencia en las pruebas realizadas.

Tomando en cuenta los tiempos de envío del primer y último mensaje en el caso de un solo nodo con un periodo de transmisión dado, se puede calcular la cantidad máxima de bits por segundo que fue posible enviar para este periodo. A partir de este resultado se puede definir como eficiencia relativa: el porcentaje máximo de carga útil enviada por segundo. También puede decirse que es el porcentaje de ancho de banda utilizado. La Tabla XVIII muestra como esta eficiencia relativa es significativamente mayor para el caso de mensajes de mayor tamaño, debido a que el retraso principal en los mensajes está dedicado a la creación de los encabezados de cada una de las capas, de manera que toma aproximadamente el mismo tiempo realizar el envío de una carga útil de tamaño máximo que el de una de tamaño mínimo. Además puede observarse que el ancho de banda de 250 kbps no es utilizado ni siquiera en un 6% para cualquier caso ya que la cantidad máxima de bits transmitidos es de 13.4 kbps.

Tabla XVIII. Comparación de Eficiencia Relativa

Tx	Msjs	Bytes de carga útil	Delta de tiempo (pqt1999-pqt0)	Eficiencia 1000 msjs	Eficiencia relativa	Bits por segundo
Mínima Carga Útil 5 ms	264	1056	6.483	13.79%	2.13%	9447
Máxima Carga Útil 5 ms	294	23520	18.5	76.19%	4.12%	13349
Mínima Carga Útil 50 ms	1000	4000	49.103	13.79%	0.28%	4724
Máxima Carga Útil 50 ms	1000	80000	62.581	76.19%	1.22%	13422
Rx	Msjs	Bytes de carga útil	Delta de tiempo (pqt1999-pqt0)	Eficiencia 1000 msjs	Eficiencia relativa	Bits por segundo
Mínima Carga Útil 5 ms	196	784	6.483	13.79%	2.13%	7014
Máxima Carga Útil 5 ms	184	14720	18.5	76.19%	4.12%	8354
Mínima Carga Útil 50 ms	1645	6580	49.103	13.79%	0.28%	7772
Máxima Carga Útil 50 ms	683	54640	62.581	76.19%	1.22%	9167

V.3 Tamaño de mensajes

ZigBee maneja un tamaño máximo de mensaje de 128 bytes, de los cuales 25 corresponden al conjunto de encabezados de las diferentes capas sin embargo el tamaño máximo de la carga útil de la aplicación se encuentra restringido por la cantidad máxima de parámetros que llevan algunos de los comandos del ZDO y el tamaño de la trama auxiliar para el caso de paquetes con seguridad. Debido a que se utilizó esta carga útil restringida, la mayor cantidad de bytes de carga útil que pudieron ser enviados para las pruebas realizadas fue de 80 bytes, y por esta razón el tamaño mayor del paquete enviado fue de 105 bytes.

No existe duda alguna sobre la capacidad de los nodos para enviar paquetes de diferentes tamaños. Sin embargo, a partir del análisis realizado en la sección V.2, puede observarse que el retraso principal que se tiene es en la creación de encabezados del paquete, sin importar la cantidad de carga útil. Es decir, la cantidad de mensajes enviados es aproximadamente la misma, para todos los casos, a pesar de que la carga útil varíe en tamaño. Únicamente en el caso de dos nodos hijo en la red puede observarse una disminución de casi el 45% en la cantidad de mensajes enviados, debida probablemente a colisiones y no necesariamente al tamaño del mensaje.

Al observar los resultados de la Tabla XVIII puede concluirse que el protocolo ZigBee tiene mejores capacidades para el envío de mensajes largos debido a que a pesar de tomar 27% más tiempo para enviar aproximadamente la misma cantidad de mensajes, fue capaz de enviar 2.8 veces más bytes de carga útil que en el caso de los mensajes de tamaño mínimo. Las aplicaciones de monitoreo con una carga útil mayor en los mensajes se beneficiarán de ésta característica.

V.4 Redundancia

Una de las características más importantes que ofrece el protocolo ZigBee es el enrutamiento malla, lo cual permite dar respuesta a una de las necesidades prioritarias de los requerimientos de la ISA. En comparación con los protocolos utilizados en redes cableadas de sensores, esta característica demuestra una ventaja considerable para ZigBee, debido a que a excepción de Industrial Ethernet, los protocolos estudiados no cuentan con la capacidad de búsqueda de una nueva ruta para los mensajes después de detectar una falla. Sin embargo esta ventaja tiene también un costo en tiempo de respuesta, debido a que la recuperación de la ruta no puede realizarse en forma instantánea, toda aplicación que pretenda utilizarla, deberá tomar en cuenta el costo en tiempo de la búsqueda de una nueva ruta. Por esta razón se realizó la Prueba 6 *Tiempo de recuperación de ruta - Redundancia.*, en la cual puede observarse el funcionamiento del enrutamiento malla en una red sencilla.

La Prueba 6 supone el buen funcionamiento del enrutamiento malla del protocolo y únicamente mide el retraso debido a la detección y búsqueda de la ruta nueva. La Figura 15 muestra el tiempo de retraso debido a la búsqueda de una nueva ruta para enviar mensajes con carga útil máxima y mínima.

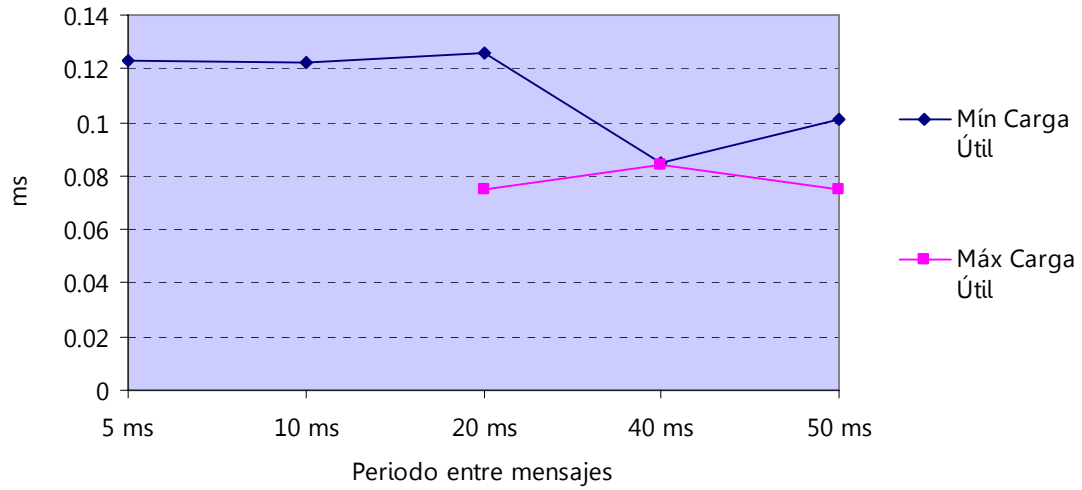


Figura 15. Resultados de la Prueba 6 Tiempo de recuperación de ruta – Redundancia

Como puede observarse el retraso es mayor en el caso de un periodo de envío de mensajes más pequeño para una carga útil mínima. Para la carga útil máxima no fue posible la recuperación de la ruta en los periodos de 5 y 10 milisegundos, esto se debe a la sobrecarga de tareas con que cuenta el nodo durante la búsqueda de la nueva ruta. El dato más sobresaliente en esta prueba es

que el mayor retraso es de aproximadamente 15 ms en una red pequeña de 4 nodos como se definió en la Prueba 6 de manera que la búsqueda de la ruta implica que los mensajes viajen sólo dos saltos de profundidad. Por lo tanto los requerimientos de cualquier aplicación en que se utilice este protocolo no deben verse afectados por este retraso. De acuerdo a los resultados de la Prueba 9 *Tamaño de la red – Capacidad máxima* el promedio de tiempo para la búsqueda de una ruta en una red de 32 nodos es de 58 ms. Para enviar un mensaje, encontrando una ruta de costo[6] 1, este tiempo de respuesta se alarga debido a la necesidad de todos los nodos presentes de enviar su respuesta al nodo central. La gran cantidad de colisiones y reintentos de envíos retrasan en gran medida la respuesta de un enrutamiento. Por esta razón, se propone el uso del protocolo ZigBee en redes con densidad baja de enrutadores.

V.5 Número de Dispositivos

El tamaño de la red puede afectarla en diferentes etapas. Al momento de creación de la red, el tiempo para su instalación depende en gran medida de la cantidad de nodos que deben ser conectados. Una vez conectada la red, el tamaño determina la posibilidad de colisiones y el retraso en el envío de mensajes, debido a la necesidad de realizar varios intentos para ganar el canal. Además existe un máximo posible de transmisiones debido a que el ancho de banda disponible

[6] Costo se define como el número de saltos que tendrán que dar los mensajes enviados a través de esa ruta.

deberá ser utilizado por una cantidad mayor de dispositivos. De acuerdo a la especificación del protocolo ZigBee es posible obtener tamaños de red de hasta 65000 dispositivos. A continuación se describen algunas razones por las cuales la implementación de redes de gran tamaño puede ser altamente compleja, lenta e incluso imposible, debido a los tiempos necesarios de conexión e instalación y a las restricciones físicas de ancho de banda del protocolo.

Debe tomarse en cuenta que el número de dispositivos dado por el estándar se refiere principalmente a la posibilidad de obtener direcciones de 16 bits únicas para los nodos dentro de la red, en cuyo caso el número total de posibles direcciones sería 65536. De acuerdo a un estudio realizado en (Sun, 2006) al ancho de banda de 250 kbps deben restársele los bits por segundo enviados en encabezados y *acknowledgements* para calcular el ancho de banda útil del protocolo. Además debe agregarse a la fórmula el tiempo de espera necesario para el cambio de modo del radio y el tiempo entre envío de tramas. Con estos datos en cuenta en (Skogholt, 2006) se calcula un ancho de banda máximo de 142.86 kbps de carga útil, para un nodo transmitiendo 96 bytes de carga útil y 30 de encabezados en cada mensaje y con un *acknowledgement* de 5 bytes. De manera que suponiendo una tasa de datos de 3 kbps por nodo se podrían tener a lo más 47 nodos en un mismo canal. Utilizando las mismas fórmulas de (Sun, 2006) es posible calcular el ancho de banda útil máximo para ZigBee. A continuación se muestra la formula utilizada en (Sun, 2006) para el cálculo del ancho de banda, dónde C_p es la tasa de datos definida por el protocolo, S_{packet}, S_{ack} y S_{header} son los

tamaños en bits de la carga útil, el *acknowledgement* y los encabezados respectivamente. T_{wait} es el tiempo de espera especial mencionado anteriormente para el cambio de modo en el radio y el tiempo entre tramas.

(1) $C_p = 250 \ kbps$

(2) $S_{packet} = 824 \ bits$

(3) $S_{ack} = 40 \ bits$

(4) $S_{header} = 200 \ bits$

(5) $T_{wait} = 1.152 \ ms$

(6) $T_{packet} = \frac{S_{packet}}{C_p}$

(7) $T_{ack} = \frac{S_{ack}}{C_p}$

(8) $T_{header} = \frac{S_{header}}{C_p}$

(9) $C_{ZigBee} = \frac{T_{packet}}{T_{packet} + T_{header} + T_{ack} + T_{wait}} \ x \ C_p = 152.37 \ kbps$

Como puede observarse el ancho de banda útil para ZigBee es de 152.37 kbps. Ahora bien, si se toma en cuenta que en la Prueba 1 *Integridad de los datos - Estrella***,** se utilizan a lo más 6 nodos transmisores, el ancho de banda útil calculado debe dividirse entre éstos, con lo cual se obtiene un ancho de banda de 25.4 kbps máximo para cada nodo. Al igual que en (Skogholt, 2006) es importante resaltar el hecho de que este valor en la práctica puede resultar mucho menor debido a que no se toman en cuenta colisiones y tiempos de *back off* del protocolo MAC. Este fenómeno puede observarse en los resultados de la sección V.1 Ancho de Banda.

Por otro lado en la Prueba 7 *Tiempo de Conexión* se muestra el efecto del tamaño de la red en el tiempo de conexión de los nodos. Como puede observarse la unión de un nuevo nodo a la red toma un tiempo mayor, debido a la existencia de más nodos y al retraso que sus respuestas provocan.

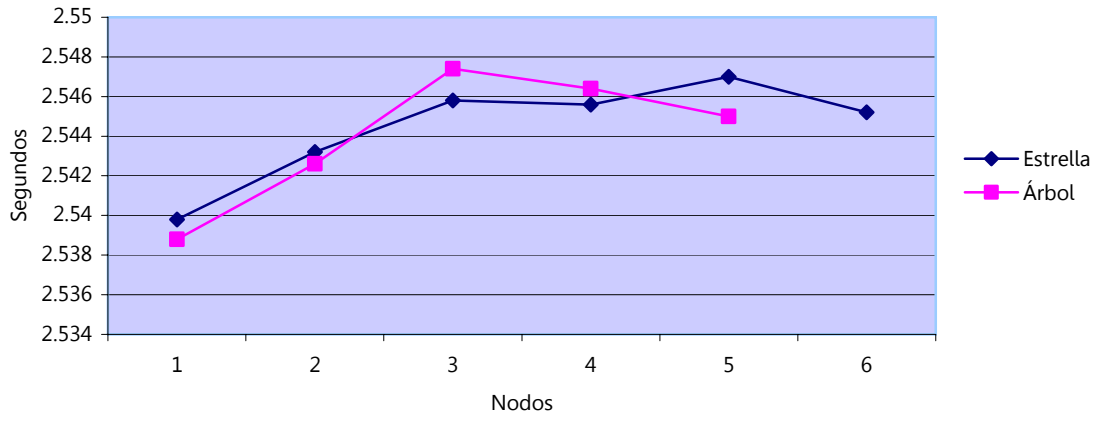


Figura 16. Comparación de los tiempos de conexión de las topologías estrella y árbol con ZRs, obtenidos en la realización de la *Prueba 7. Tiempo de Conexión*

Como puede observarse, el tiempo de conexión de un nuevo nodo aumenta en ambas topologías al menos hasta tener 3 nodos, y de 4 a 6 nodos aunque disminuye un poco para el caso de la topología árbol, sigue siendo bastante mayor que los tiempos de conexión de 1 y 2 nodos. Este fenómeno se debe a que la cercanía entre los nodos permite que reciban mensajes de cualquier otro nodo en la red. En ambas topologías se explica el retraso debido a que el proceso de conexión del nuevo nodo requiere recibir respuestas de todos los nodos FFD existentes, analizarlas y elegir al mejor candidato para intentar la unión. Por otro lado, la disminución del tiempo a partir de 4 nodos puede deberse a que el tiempo para recepción de *beacons* de los otros nodos, es fijo y no es suficiente para recibir las respuestas de más de 3 nodos.

En la Figura 17 se muestra el tiempo de conexión obtenido utilizando únicamente ZEDs para la red estrella. En este caso el tiempo de conexión no varía conforme crece el tamaño de la red, debido a que el único nodo capaz de responder a la petición de unión de un nuevo nodo es el coordinador. Se muestran dos picos en los nodos 4 y 7, esto se debe a que en ambos casos se realizaron dos intentos de búsqueda de redes lo cual genera un retraso de apenas 10 ms, lo que equivale al 4% del tiempo total de conexión.

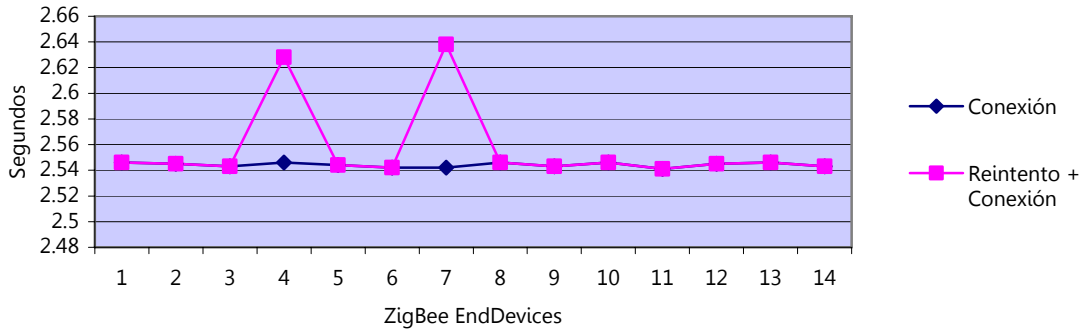


Figura 17. Tiempo de conexión en topología estrella de ZEDs, obtenidos en la *Prueba 7. Tiempos de Conexión.*

Como puede observarse el principal problema del tiempo de conexión es que en el caso de una red de tantos nodos como los que supone usar ZigBee, por ejemplo la conexión consecutiva de 65000 nodos sin reintentos tomaría aproximadamente 46 horas 26 minutos. Sin embargo, es posible reducir este tiempo tratando de unir la mayor cantidad posible de nodos, iniciando el proceso de conexión casi simultáneamente. Para observar el comportamiento del protocolo en esta situación se realizó la Prueba 8 ***Conexiones simultaneas***. Los resultados se muestran en la Figura 18.

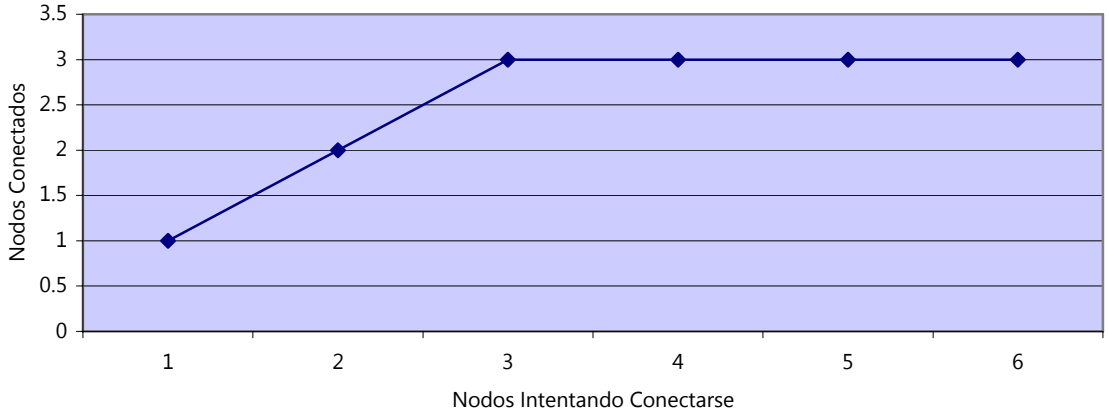


Figura 18. Número máximo de conexiones simultáneas exitosas

La Prueba 8, como se le define en el Capítulo IV, consistió en encender al mismo tiempo cierta cantidad de nodos, para que el inicio de su proceso de unión también fuera simultáneo. El resultado de esta prueba muestra un pequeño fallo en el diseño del proceso de unión a la red, que sólo permite la unión simultánea de 3 nodos máximo. Para explicar mejor este resultado en la Figura 19 se muestra la captura del analizador de red.

Seq No	Channel	Time	Time Delta	MAC Src	MAC Dest	N.	Protocol	Packet Type
1	26	23:19:38.000			0xffff		IEEE 802.15.4	Command: Beacon Request
2	26	23:20:21.293	+00:00:43.293		0xffff		IEEE 802.15.4	Command: Beacon Request
3	26	23:20:21.295	+00:00:00.002	0x0000			IEEE 802.15.4	Beacon: BO: 15, SO: 15, PC: 1,
4	26	23:20:21.365	+00:00:00.070		0xffff		IEEE 802.15.4	Command: Beacon Request
5	26	23:20:21.370	+00:00:00.005	0x0000			IEEE 802.15.4	Beacon: BO: 15, SO: 15, PC: 1,
6	26	23:20:21.424	+00:00:00.054		0xffff		IEEE 802.15.4	Command: Beacon Request
7	26	23:20:21.428	+00:00:00.004	0x0000			IEEE 802.15.4	Beacon: BO: 15, SO: 15, PC: 1,
8	26	23:20:21.505	+00:00:00.077		0xffff		IEEE 802.15.4	Command: Beacon Request
9	26	23:20:21.508	+00:00:00.003	0x0000			IEEE 802.15.4	Beacon: BO: 15, SO: 15, PC: 1,
10	26	23:20:21.510	+00:00:00.002		0xffff		IEEE 802.15.4	Command: Beacon Request
11	26	23:20:21.514	+00:00:00.004	0x0000			IEEE 802.15.4	Beacon: BO: 15, SO: 15, PC: 1,
12	26	23:20:23.331	+00:00:01.817	0x0500000000000000	0x0000		IEEE 802.15.4	Command: Association Request
13	26	23:20:23.332	+00:00:00.001				IEEE 802.15.4	Acknowledgment
14	26	23:20:23.403	+00:00:00.071	0x0100000000000000	0x0000		IEEE 802.15.4	Command: Association Request
15	26	23:20:23.404	+00:00:00.001				IEEE 802.15.4	Acknowledgment
16	26	23:20:23.463	+00:00:00.059	0x0300000000000000	0x0000		IEEE 802.15.4	Command: Association Request
17	26	23:20:23.464	+00:00:00.001				IEEE 802.15.4	Acknowledgment
18	26	23:20:23.544	+00:00:00.080	0x0400000000000000	0x0000		IEEE 802.15.4	Command: Association Request
19	26	23:20:23.544	+00:00:00.001				IEEE 802.15.4	Acknowledgment
20	26	23:20:23.550	+00:00:00.006	0x0200000000000000	0x0000		IEEE 802.15.4	Command: Association Request
21	26	23:20:23.550	+00:00:00.001				IEEE 802.15.4	Acknowledgment
22	26	23:20:23.827	+00:00:00.277	0x0500000000000000	0x0000		IEEE 802.15.4	Command: Data Request
23	26	23:20:23.828	+00:00:00.001				IEEE 802.15.4	Acknowledgment
24	26	23:20:23.832	+00:00:00.005	0xaaaaaaaaaaaaaaaa	0x0500000000000000		IEEE 802.15.4	Command: Association Response
25	26	23:20:23.833	+00:00:00.001				IEEE 802.15.4	Acknowledgment
26	26	23:20:23.897	+00:00:00.063	0x0100000000000000	0x0000		IEEE 802.15.4	Command: Data Request
27	26	23:20:23.897	+00:00:00.001				IEEE 802.15.4	Acknowledgment
28	26	23:20:23.902	+00:00:00.005	0xaaaaaaaaaaaaaaaa	0x0100000000000000		IEEE 802.15.4	Command: Association Response
29	26	23:20:23.903	+00:00:00.001				IEEE 802.15.4	Acknowledgment
30	26	23:20:23.959	+00:00:00.056	0x0300000000000000	0x0000		IEEE 802.15.4	Command: Data Request
31	26	23:20:23.960	+00:00:00.001				IEEE 802.15.4	Acknowledgment
32	26	23:20:23.965	+00:00:00.005	0xaaaaaaaaaaaaaaaa	0x0300000000000000		IEEE 802.15.4	Command: Association Response
33	26	23:20:23.966	+00:00:00.001				IEEE 802.15.4	Acknowledgment
34	26	23:20:24.038	+00:00:00.073	0x0400000000000000	0x0000		IEEE 802.15.4	Command: Data Request
35	26	23:20:24.039	+00:00:00.001				IEEE 802.15.4	Acknowledgment
36	26	23:20:24.044	+00:00:00.006	0x0200000000000000	0x0000		IEEE 802.15.4	Command: Data Request
37	26	23:20:24.045	+00:00:00.001				IEEE 802.15.4	Acknowledgment

Figura 19. Proceso de conexión simultanea de 5 nodos

En la Figura 19 se muestra el caso en que se conectan 5 nodos simultáneamente. Del paquete con número de secuencia 1 al 10 puede observarse que los 5 nodos realizan la búsqueda de redes para unirse y las respuestas a cada uno desde el ZC. Posteriormente del paquete 12 al 23 se puede ver que cada nodo inicia el proceso de conexión enviando el comando *Association Request.* El nodo coordinador da respuesta a las primeras 3 peticiones de conexión recibidas enviando los *Association Response* en los paquetes 24, 28 y 32, pero no es capaz

de responder las dos siguientes. Después de esto los últimos dos nodos no realizan de nuevo un intento de conexión, debido a que no existe ningún tiempo máximo de espera por la respuesta. Este comportamiento no permite la conexión simultánea de más de 3 nodos, por lo que se recomienda esperar al menos 2 segundos, tiempo necesario para terminar de conectar los 3 nodos simultáneamente, antes de intentar conectar más nodos. También debe notarse que la conexión simultánea reduce a 1 tercio el tiempo total de conexión calculado previamente para 65000 nodos. En el caso de la prueba con una red densa, se lograron conectar 32 nodos en un tiempo total de 5 minutos y 43.831 segundos, sin embargo esta red no requirió de ningún tipo de configuración especial. Si se toma en cuenta que el diseño e instalación física de las rutas de cableado de cualquier tipo de red de sensores cableada, puede durar incluso varios días para lograr un diseño apropiado de conexión e instalación de una red de 32 nodos, se puede decir que los tiempos de conexión del protocolo ZigBee son una ventaja notable.

Los resultados previos muestran una de las ventajas más obvias e importantes de las redes inalámbricas de sensores para aplicaciones en ambientes industriales. Debido a que el ahorro en tiempos de configuración e instalación de la red de sensores puede ayudar a disminuir costos de producción.

V.6 Respuesta en tiempo y variación multisalto.

Además del tiempo de procesamiento del mensaje, existen dos factores importantes que determinan el tiempo de respuesta de un dispositivo en una red: la distancia y el número de saltos que debe viajar un mensaje para llegar a su destino. En la Prueba 5 *Tiempo de respuesta – Multisalto.*, se muestra el retraso que un número determinado de saltos provoca en la respuesta del mensaje.

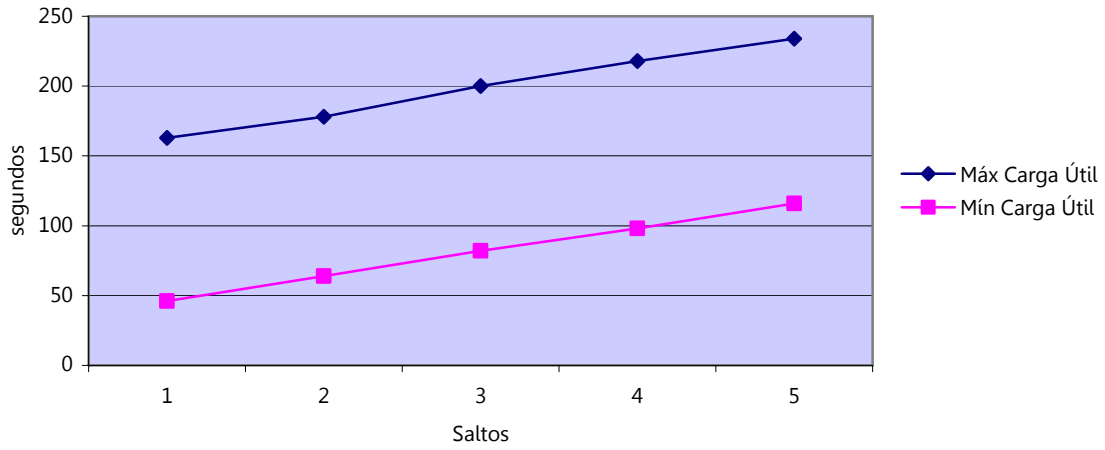


Figura 20. Tiempo de respuesta multisalto

Como puede observarse, el tiempo de respuesta crece en forma lineal con el número de saltos que necesita el mensaje para llegar al dispositivo destino. Además debe notarse que el tiempo de retraso promedio introducido por cada salto dentro de la ruta es de 17.5 ms para una carga útil mínima. Lo cual restringe

el tipo de aplicaciones en que se pueden utilizar estos dispositivos, ya sea conectándolos en una profundidad adecuada que les permita responder con prontitud suficiente o utilizando únicamente redes tipo estrella. Es decir, o bien se utilizan dispositivos con profundidad 1 en una red estrella, o se asegura que la suma total de retrasos se encuentre dentro del tiempo requerido para la aplicación.

Además puede observarse una vez más el fenómeno de triplicación del tiempo de transmisión cuando ésta contiene una carga útil máxima. Sin embargo la retransmisión del mensaje por los nodos intermedios no aumenta de ésta manera manteniéndose un retraso promedio de 17.75 ms por cada salto dentro de la ruta. El hecho de que la retransmisión de mensajes no implique un mayor retraso cuando la carga útil es mayor de nuevo demuestra que la causa principal del retraso está en el paso del mensaje a las capas superiores de la arquitectura.

V.7 Respuesta en tiempo y variación con la distancia.

Para observar el efecto de la distancia en el tiempo de respuesta se realizaron dos pruebas, una en un ambiente exterior (al aire libre) y otra en un ambiente interior, para la prueba al aire libre el lugar elegido fue un estacionamiento de Oceanología del centro de investigación (CICESE), pero la prueba se realizó durante las horas en que se encuentra vacío, para evitar lo más posible fenómenos como interferencias, multitrayectorias, etc. Como puede

observarse en la Figura 21, el retraso no tiene dependencia del periodo de transmisión de los mensajes.

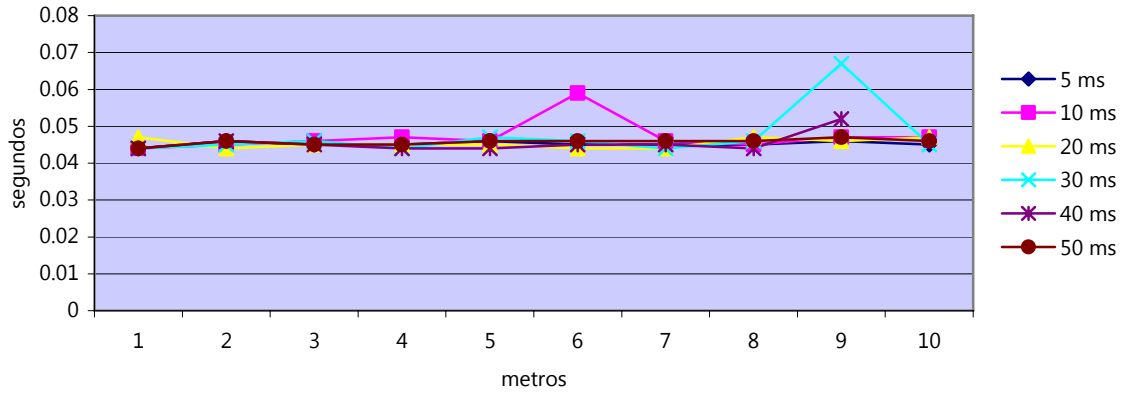


Figura 21. Resultados de la *Prueba 4 Tiempo de respuesta – Distancia*. Prueba realizada en un ambiente exterior y variando el periodo de transmisión de los mensajes

Además puede observarse que aunque en la mayoría de los casos no existe una variación significativa al aumentar la distancia, los más altos valores de retraso se encuentran en distancias mayores a 5 metros. Posteriormente se realizó la misma prueba con los nodos a 1m de altura del piso con lo cual se obtuvieron los resultados de la Figura 22. Puede observarse nuevamente que no existe un retraso significativo en el tiempo de respuesta al aumentar la distancia. Es posible también que el retraso no sea notorio debido a que el rango mínimo ofrecido por la herramienta de medición de los tiempo es de 1 ms. Por lo que diferencias menores a éste valor no pueden ser mostradas.

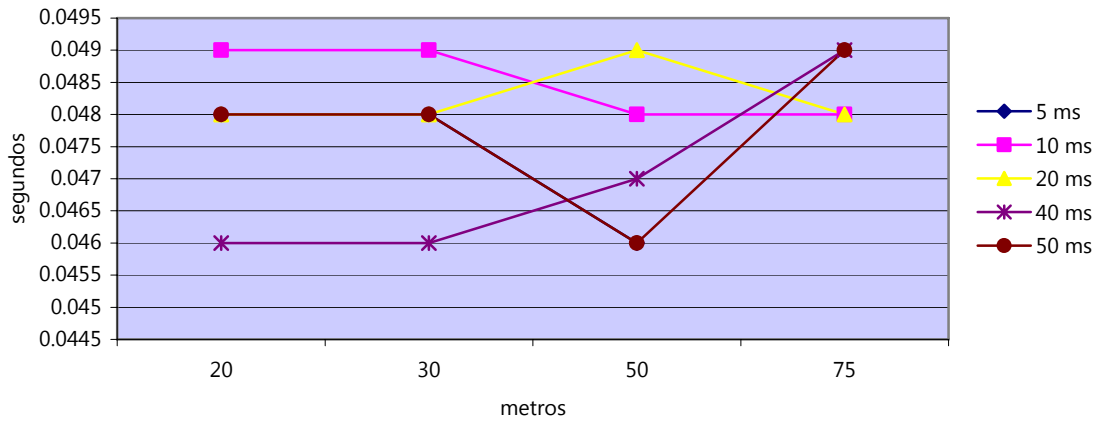


Figura 22. Resultados de la Prueba 4 *Tiempo de respuesta – Distancia,* colocando los nodos a 1m de altura sobre el piso

En la Figura 23 se muestran los valores promedio y máximos para la prueba al aire libre, se puede observar que el mayor tiempo de respuesta son 67 ms mientras que el menor 44 ms, por lo que se tiene una diferencia de 23 ms en el peor de los casos, y por lo tanto en el peor caso un retraso del 52.27% del tiempo máximo de envío del mensaje.

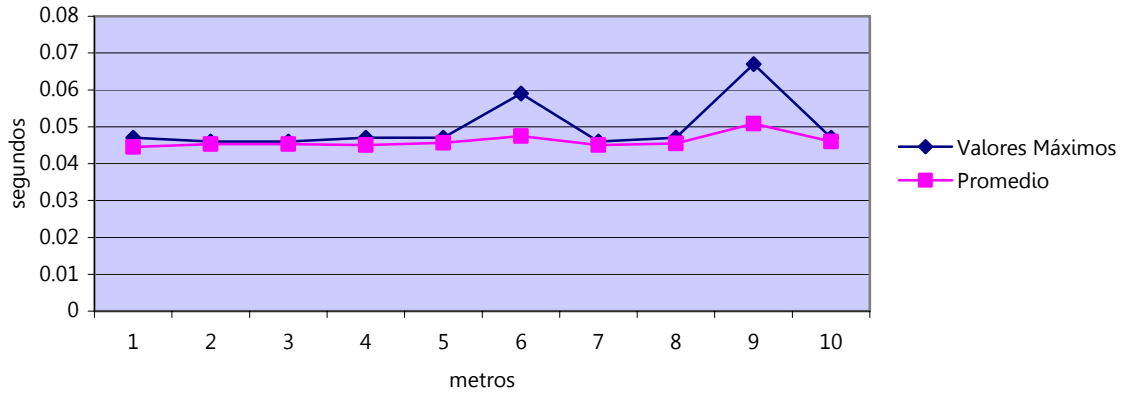


Figura 23. Resultados máximo y promedio de la *Prueba 4 Tiempo de respuesta – Distancia*. Prueba realizada en un ambiente exterior y variando el periodo de transmisión de los mensajes

El otro caso de pruebas fue realizado en el interior del edificio de la División de Física Aplicada del CICESE, en el pasillo del tercer piso. Como puede observarse en este caso se pudo conseguir una mayor distancia para la recepción de mensajes, lo que probablemente se debe al entorno físico del pasillo (puertas cerradas, sin obstáculos y con línea de vista entre los nodos) que permitió un mayor número de trayectorias en la transmisión de los mensajes. Por lo que se muestran resultados hasta 20 metros en la Figura 24 y la Figura 25. Nuevamente se puede observar que el retraso no se encuentra afectado por el periodo de envío de mensajes, pero también se observa que la diferencia entre el tiempo de respuesta máximo de 50 ms y el mínimo de 46 ms es de tan solo 4 ms y no representa más del 8.7% del tiempo total de retraso mínimo.

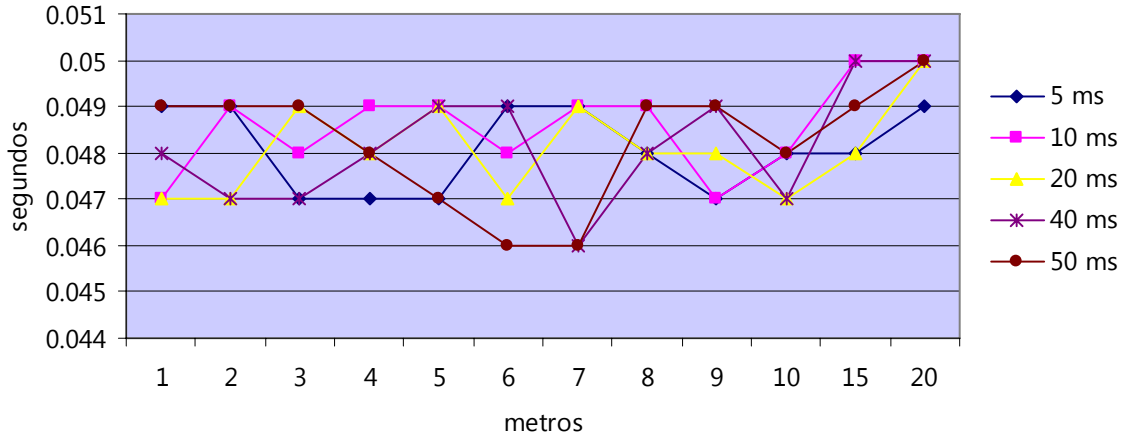


Figura 24. Resultados de la *Prueba 4 Tiempo de respuesta – Distancia*. Prueba realizada en un ambiente interior y variando el periodo de transmisión de los mensajes

En la Figura 25 se muestran los valores máximo y promedio para cada distancia, puede observarse la uniformidad de éstos valores con la distancia, y un ligero incremento de apenas 1 ms para más de 10 metros de distancia. Es posible que este incremento sea ligeramente mayor a 1 ms, sin embargo la unidad mínima en tiempo que el analizador de redes utilizado puede capturar es 1 ms.

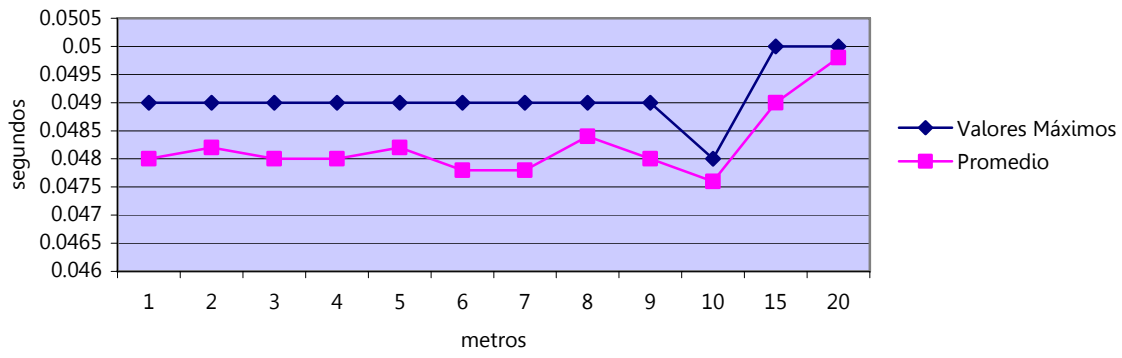


Figura 25. Resultados máximo y promedio de la *Prueba 4 Tiempo de respuesta – Distancia*. Prueba realizada en un ambiente interior y variando el periodo de transmisión de los mensajes

V.8 Integridad de los datos

Existen varias causas por las que la integridad de los datos se puede ver comprometida. Entre estas causa se encuentran el nivel de ruido en el canal de transmisión, las pérdidas de potencia al aumentar la distancia o bien las fallas en la retransmisión de mensajes a través de varios saltos. No se realizaron pruebas de nivel de ruido, debido a que este factor es sumamente variable y no podría generalizarse un nivel de ruido para aplicaciones industriales. Sin embargo, se trató de evitar lo más posible interferencias en las pruebas, se verificó que no existieran redes 802.15.4 en la cercanía de las pruebas realizadas, y se utilizó el canal 26 para evitar la interferencia de redes 802.11. Todo esto con la finalidad de observar las pérdidas de datos al modificar otros factores como son: la distancia, el ambiente

físico, el número de saltos, el periodo de transmisión y el tamaño de los mensajes enviados.

En cuanto a la variación en la distancia, la respuesta del dispositivo se encuentra fuertemente ligada al tipo de hardware utilizado. Para la Prueba 3 ***Integridad de los datos - Distancia*** se utilizaron módulos Panasonic PAN802154HAR00, en la Figura 26 se muestra el efecto de la distancia en la transmisión y recepción de mensajes en una red instalada en el exterior.

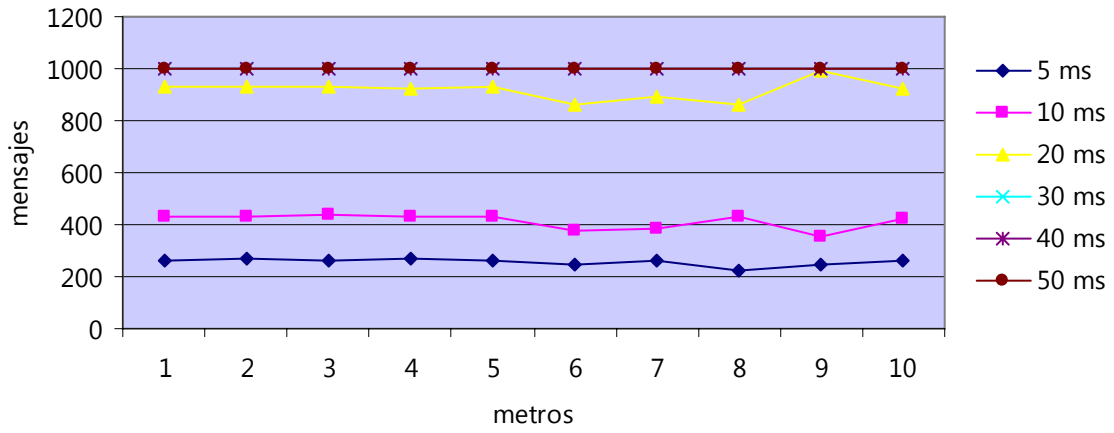


Figura 26. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes enviados en un ambiente exterior

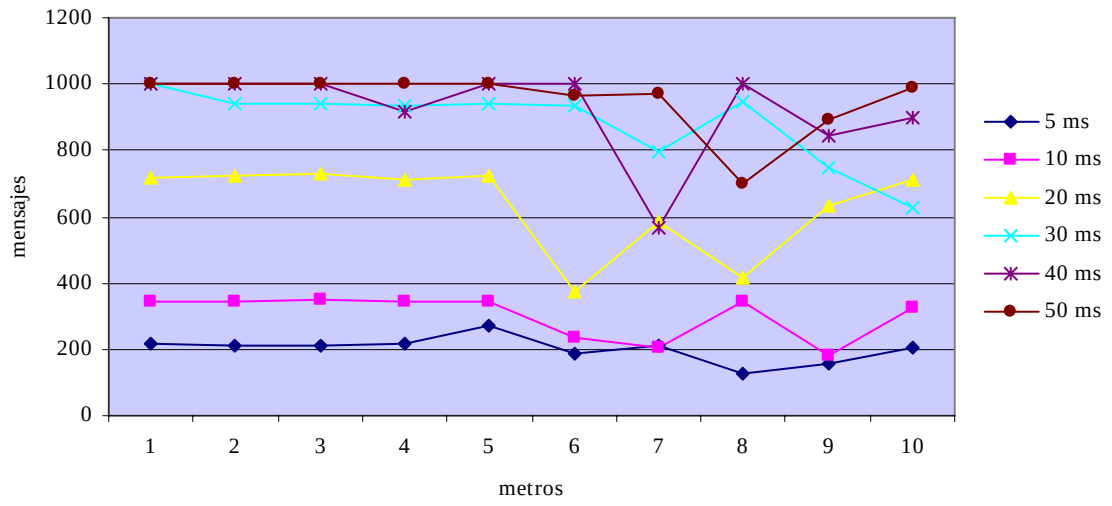


Figura 27. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes recibidos en un ambiente exterior

El número de mensajes enviados varía ligeramente en la transmisión debido al aumento de reenvíos por la falta de *acknowledgements*. Para esta prueba se intentó primero el envío de mensajes a 15 metros con los nodos en el piso, pero en varios casos no fue posible que el nodo transmisor recibiera la orden para comenzar la transmisión, por lo que estos resultados no se presentan. La imposibilidad de los dispositivos para enviar con suficiente potencia el mensaje hace su desempeño insuficiente para aplicaciones en que las distancias entre los nodos sean mayores a 10metros.

Sin embargo de acuerdo al trabajo en (Tanenbaum, 2006) la distancia de transmisión varía de acuerdo a la posición del nodo. En (Tanenbaum, 2006) se asegura que elevar los nodos 1 metro sobre el piso permite aumentar la distancia

de transmisión 5 veces, por lo que la Prueba 3 *Integridad de los datos - Distancia*, se repitió elevando los nodos 1 metro para las distancias presentadas en la Figura 28 y la Figura 29.

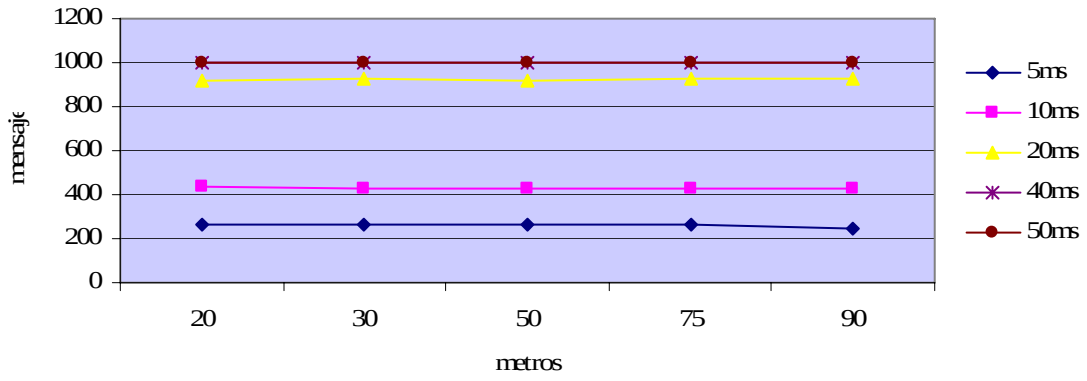


Figura 28. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes enviados en un ambiente exterior, elevando los nodos a 1m de altura del piso

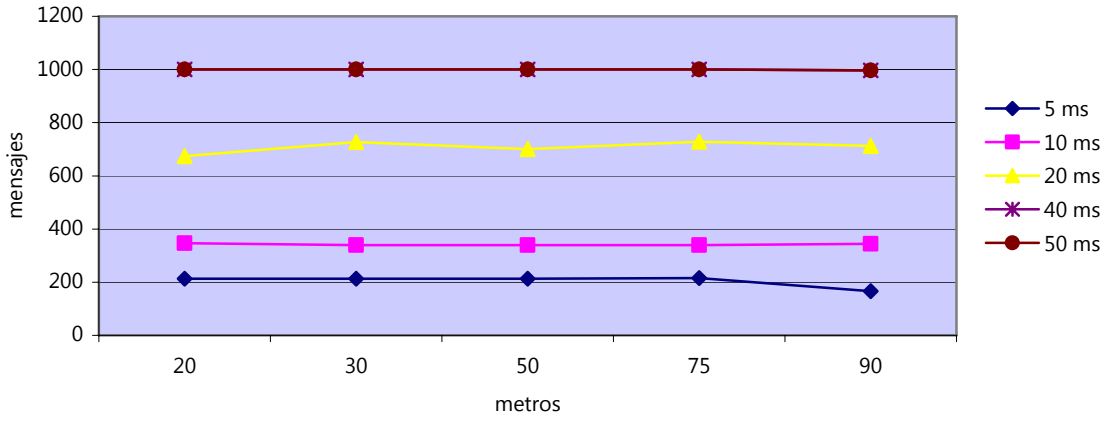


Figura 29. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes recibidos en un ambiente exterior, elevando los nodos a 1 m de altura del piso

Como puede observarse en la Figura 28 y en la Figura 29 no existen pérdidas significativas en la cantidad de mensajes recibidos o transmitidos, incluso más allá de la distancia máxima especificada para el protocolo a 75 m y 90 m.

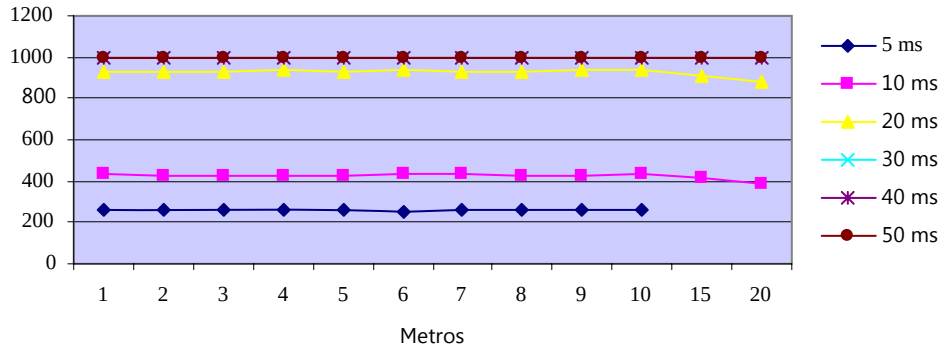


Figura 30. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes enviados en un ambiente interior

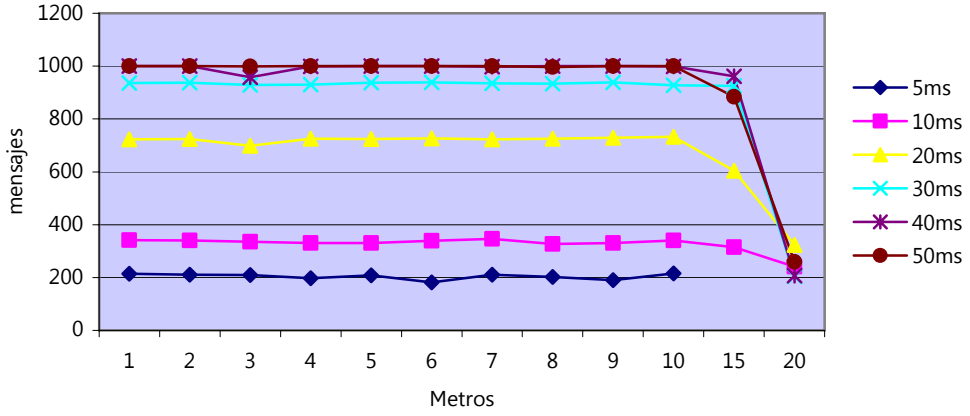


Figura 31. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes recibidos en un ambiente interior

Tanto en este caso como en el de la Prueba 4 de variación del tiempo de respuesta con la distancia el desempeño resulta mejor en ambientes cerrados, como se muestra en la Figura 31. Sin embargo, en el caso de ambientes industriales debe tomarse en cuenta la posibilidad de existencia de otras redes que funcionen en la misma frecuencia y las posibles colisiones que estas generarían. Es mucho más común que en ambientes cerrados como plantas industriales se cuente con redes WiFi o bien algún otro tipo de fuente de ruido que impida el óptimo desempeño de la red ZigBee. En todo caso los nodos ZigBee están capacitados para elegir el canal con menor nivel de ruido durante el proceso de formación y unión, así como para unirse al dispositivo con el cual su nivel de calidad de enlace (LQI por sus siglas en inglés) sea el mejor, de entre todos los nodos a los que puede unirse. Respecto a esto debe tomarse en cuenta que la calidad del enlace puede variar así como las condiciones de ruido del ambiente, en cuyo caso las únicas características de ZigBee que pueden ayudar son las de descubrimiento de rutas y de dispositivos, para lo cual será necesario el uso de enrutamiento malla.

Se debe enfatizar que los resultados de estas pruebas se encuentran fuertemente ligados a los elementos de hardware utilizados y a las características específicas de los ambientes en que se realizaron las pruebas. El mismo protocolo en dispositivos de mayor alcance obviamente mostrará mejora en los resultados. Como puede observarse en la Figura 32 y la Figura 33 que presentan los resultados de la Prueba 3 utilizando nodos 13192-EVB de Freescale las pérdidas a distancias de 20 metros son mucho menores.

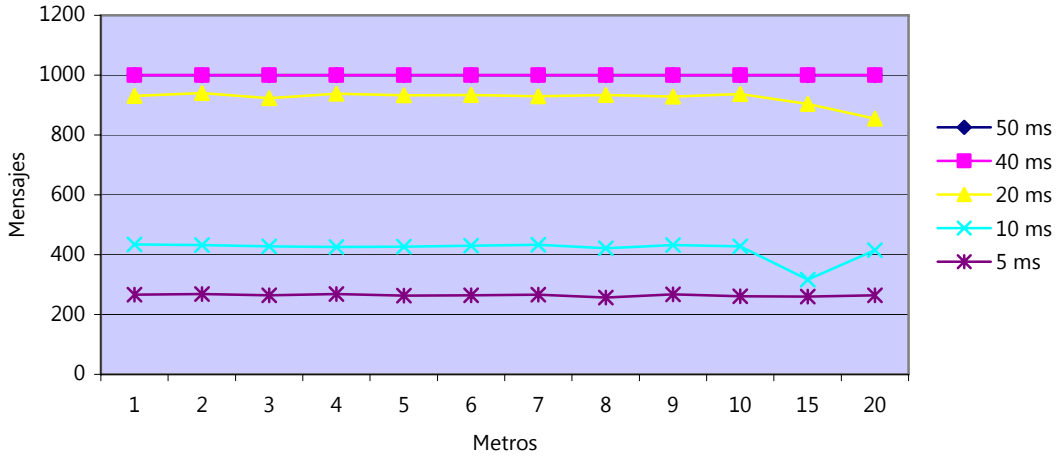


Figura 32. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes con mínima carga útil, enviados en un ambiente interior y utilizando dispositivos EVB

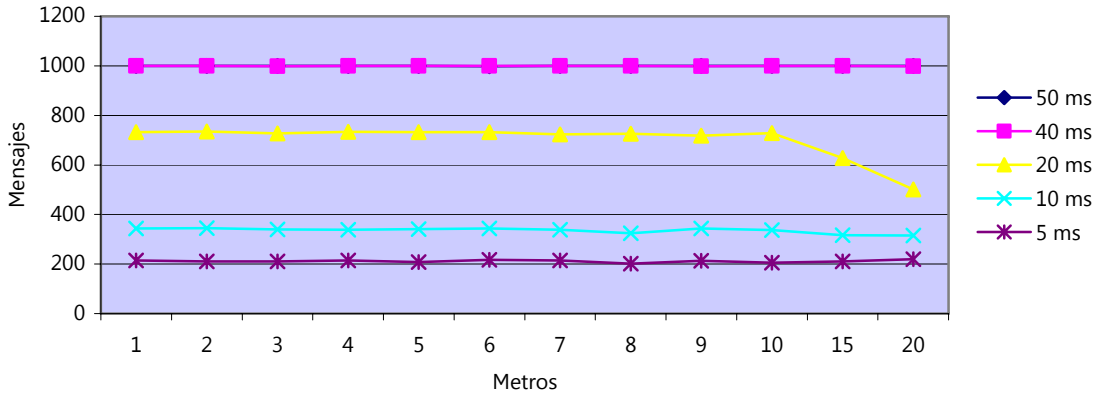


Figura 33. Resultados de la *Prueba 3. Integridad de los datos – Distancia.* Se muestra la cantidad de mensajes con mínima carga útil, recibidos en un ambiente interior y utilizando dispositivos EVB

A partir de los resultados obtenidos puede concluirse que los nodos utilizados funcionan mejor en distancias menores a 15 metros, con una carga útil mínima y en ambientes cerrados. Y con un periodo de transmisión mínimo de 40 ms.

Para el caso de las pérdidas de mensajes debidas a transmisiones multisalto se puede ver la Figura 34 y la Figura 35 que muestran los casos para una carga útil mínima.

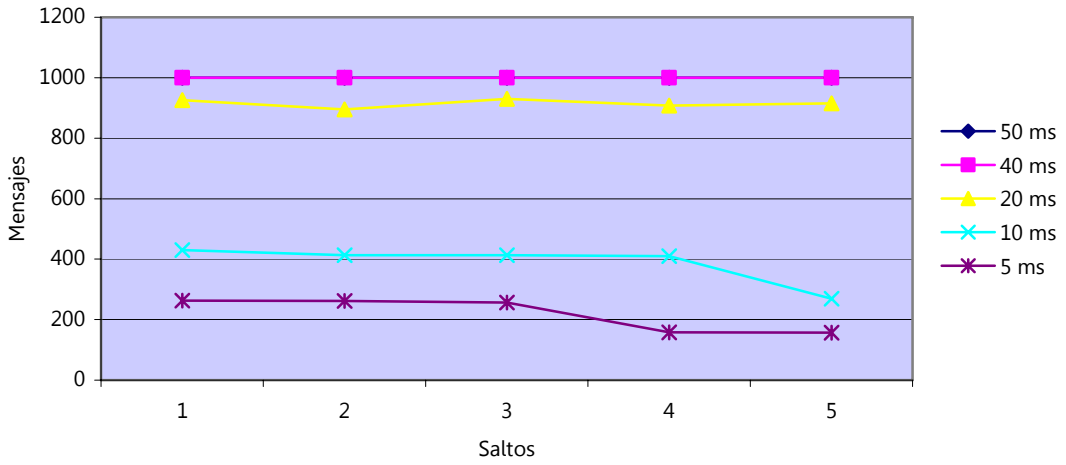


Figura 34. Resultados de la Prueba 2. Integridad de los datos – Multisalto. Se muestra la cantidad de mensajes transmitidos con mínima carga útil

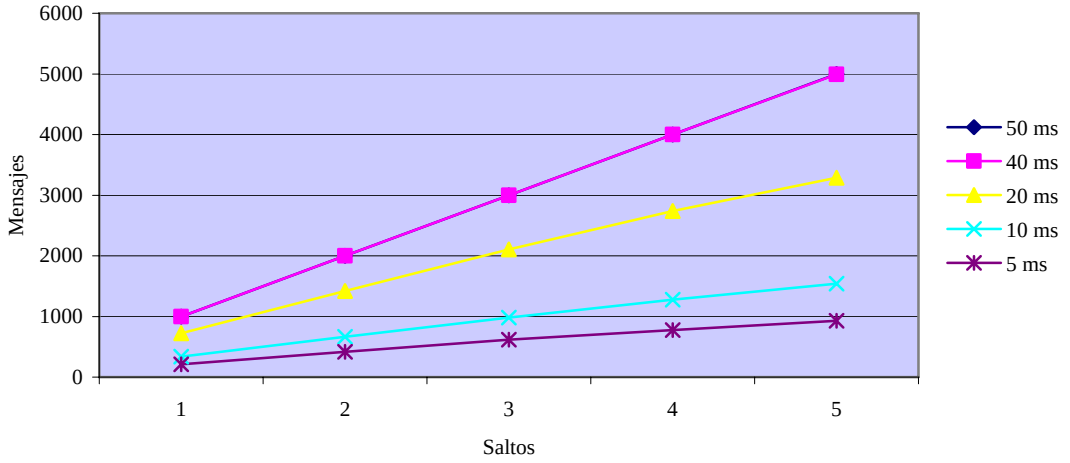


Figura 35. Resultados de la *Prueba 2. Integridad de los datos – Multisalto.* Se muestra la cantidad total de mensajes, con mínima carga útil, recibidos por el coordinador

En este caso para una carga útil de tamaño mínimo los periodos de transmisión de 40 y 50 milisegundos se logró enviar la totalidad de los mensajes o con una pérdida máxima de 1 mensaje, sin embargo en el caso de la carga útil de tamaño máximo mostrado en la Figura 37 puede observarse que para el periodo de transmisión de 50 ms se perdieron varios mensajes cuando estos viajaban más de 3 saltos esto puede deberse al retraso en conjunto ocasionado por el tamaño del mensaje y la cantidad de saltos que viaja.

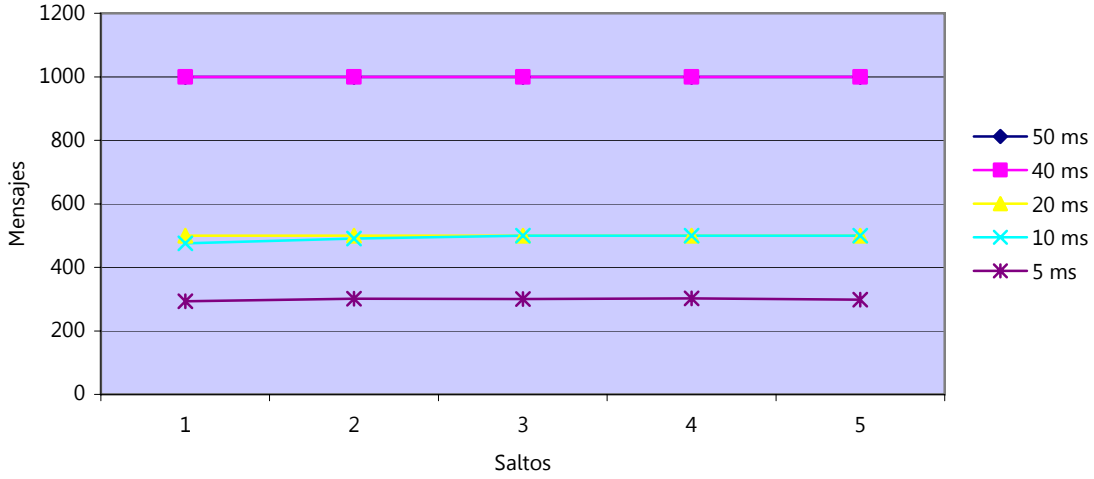


Figura 36. Resultados de la *Prueba 2. Integridad de los datos – Multisalto.* Se muestra la cantidad de mensajes enviados con máxima carga útil

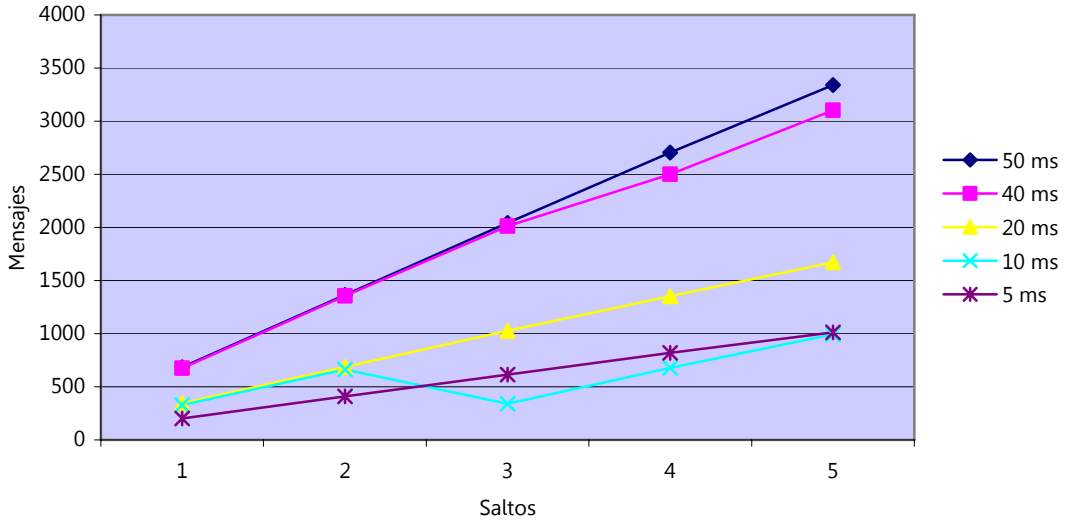


Figura 37. Resultados de la *Prueba 2. Integridad de los datos – Multisalto.* Se muestra la cantidad total de mensajes, con mínima carga útil, recibidos por el coordinador

V.9 Seguridad

Para un cifrado seguro, ZigBee especifica el uso del Estándar Avanzado de Seguridad (AES) de 128 bits. El cual consiste en la implementación del algoritmo Rijndael. Este estándar fue presentado el 26 de Noviembre del 2001 por el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) Estadounidense, como el resultado de un concurso para sustitución del antiguo método de cifrado DES.

Algunas de las características sobresalientes de éste algoritmo son presentadas en un estudio comparativo (Gladman, 1999), previo a la presentación del resultado. En primer lugar se hace notar que este algoritmo no realiza movimientos de ningún tipo en el orden de los datos, además tiene una excelente optimización en procesadores de 32 bits y cuenta con un desempeño perdurable debido a que utiliza instrucciones comúnmente disponibles en varios procesadores. Su calendarización de llave es asimétrica por lo que resulta mucho más rápido para cifrar que para descifrar. En general se le considera el mejor método presentado debido a su fácil implementación, buen desempeño al cifrar diferentes tamaños de bloques y su sencillez para ser programado en lenguaje C.

ZigBee cuenta con dos modos seguros de funcionamiento, con llave preconfigurada o sin ella. En el caso de funcionar en modo de llave no preconfigurada, después que un nodo intenta unirse a la red, el servidor de seguridad verifica que la dirección de éste no se encuentre prohibida. Si el nodo

puede ser agregado a la red se utiliza el comando *Transport Key* para enviar la llave al nodo. Durante el envío de este mensaje la llave queda expuesta y puede ser capturada para un ataque o intrusión posterior, por lo que se recomienda el uso del modo de seguridad con llave preconfigurada, en el cual para que un nodo pueda comunicarse después de unirse a la red debe tener la llave configurada desde el momento de programación de la memoria flash del mismo. De igual manera esta llave deberá guardarse en la memoria no volátil para los casos en que el nodo deba reiniciar su funcionamiento. Durante la unión con una llave preconfigurada, se realiza también el envío del comando *Transport Key*, sin df

La forma ideal del funcionamiento en modo seguro de ZigBee es inicializar la red con una llave preconfigurada, y posteriormente realizar el envío de llaves diferentes utilizando el comando *Transport Key.* Una vez enviadas las llaves puede utilizarse el número de identificación de las mismas para cambiar la llave utilizada en la comunicación con el comando Switch Key. De esta manera es posible implementar la red en modo seguro desde el principio y cambiar la llave con cierta periodicidad para evitar cualquier tipo de ataque.

El hecho de que ZigBee tenga la capacidad para cifrar mensajes utilizando uno de los algoritmos más seguros y además pueda realizar el transporte y cambio periódico de las llaves, implica el cumplimiento de varios requisitos de seguridad de la ISA. Sin embargo, debe tomarse en cuenta que la aplicación de seguridad a la red causa retrasos en el tiempo de transmisión y recepción de los mensajes,

debidos al tiempo que toma cifrarlos y descifrarlos. Además del tiempo de procesamiento también se utiliza más memoria en el nodo que funcione como dispositivo central de seguridad, de acuerdo a lo mencionado en el Capítulo III.

V.10 Topología

ZigBee cuenta con capacidad para implementar las topologías estrella, árbol y malla. La topología estrella puede formarse con un nodo coordinador y 20 nodos unidos a él en profundidad 1, de los cuales 14 pueden ser ZED o bien 6 ZR. Debe hacerse notar que si se va a utilizar una red tipo estrella, en la cual la comunicación entre los nodos hijos no es necesaria, el uso de nodos ZR resultaría en un gasto excesivo en memoria ya que toda la capacidad de enrutamiento queda desperdiciada en una topología de éste tipo. Para la topología árbol los nodos ZR tienen la capacidad de permitir a otros nodos unirse a la red a través de ellos. En este caso la capacidad de enrutamiento malla de los nodos ZR queda también desperdiciada. Sin embargo es posible agregar varios niveles de profundidad a la red que permitan alargar la distancia máxima para el envío de mensajes. Es importante aquí hacer hincapié en los resultados obtenidos en las pruebas de tiempo de respuesta e integridad de datos en multisalto, ya que como se pudo observar, el retraso en el tiempo de respuesta puede resultar significativo para algunas aplicaciones o bien la integridad de los datos puede verse afectada para cierto tamaño de mensajes.

Por último la topología malla es la capacidad más sobresaliente de éste protocolo, debido a que dota a la red con un procedimiento para auto recuperación en caso de fallo de alguna ruta, así como la búsqueda de rutas de menor costo y mejor calidad de enlace. Sin embargo no todas las aplicaciones necesitan esta capacidad y el costo de procesamiento y memoria aumenta al utilizarla. Además como pudo observarse, en la realización de las pruebas de redundancia, el tiempo de recuperación debe considerarse de acuerdo al tipo de aplicación ya que éste puede sobrepasar la necesidades de tiempo de respuesta de la red o bien dejar inutilizada la red debido al periodo o tamaño de transmisión de los mensajes.

V.11 Interoperabilidad con redes de sensores cableadas.

En la especificación del estándar de ZigBee no se encuentra definida ningún tipo de interfaz para comunicación con algún otro tipo de red. Sin embargo algunas compañías como por ejemplo en el caso de Cirronet, cuentan con dispositivos gateway para hacer posible la comunicación de dispositivos ZigBee con redes Ethernet y Modbus, como es el caso de los modelos ZG-2400M y ZG-2400E[7]. Estos dispositivos pueden integrarse a las redes cableadas para las que fueron hechos y recibir comandos de las mismas por un medio físico cableado y además, comunicarse con el protocolo ZigBee en forma inalámbrica.

[7] http://www.cirronet.com

V.12 Soporte

En cuanto al soporte técnico del protocolo una sola organización se encarga de mantenerlo actualizado, ZigBee Alliance. Sin embargo esta es probablemente una de las organizaciones más grandes entre aquellas que dan soporte a un protocolo de comunicación inalámbrica de sensores, debido a que forman parte de ella una gran cantidad de compañías que además de implementar el protocolo diseñan y fabrican productos que lo utilizan y dan soporte a desarrolladores dentro y fuera de la alianza.

En este aspecto puede decirse que ZigBee cuenta con el soporte necesario para el desarrollo de aplicaciones con base en éste protocolo, cualquier desarrollador o fabricante de dispositivos ZigBee puede contar con la información necesaria y soporte necesarios para el buen funcionamiento de su aplicación.

V.13 Método de acceso

El método de acceso de ZigBee es el especificado por el estándar IEEE 802.15.4 CSMA\CA el cual tiene una implementación sencilla y es ampliamente utilizado en diversos protocolos de comunicación. Sin embargo sufre de dos importantes problemas: el del nodo escondido y del nodo expuesto, que son los más comunes para este tipo de redes. A pesar de existir algunos métodos para solucionarlos, la implementación de éstos queda fuera del alcance del protocolo,

debido a que la especificación ZigBee se encuentra simplemente empotrada en el estándar 802.15.4 y por lo tanto se olvida de esas capas para enfocarse a las capas tres a siete.

Otro de los problemas que sufren las redes que cuentan con este tipo de métodos de acceso al medio es el de desborde o en inglés *trashing*, el cual se presenta cuando la cantidad de nodos en la red es tan grande que las colisiones, tiempo de retiro y reintentos de envío toman más tiempo y ancho de banda que el envío correcto de mensajes. Sin embargo en el caso de redes pequeñas este fenómeno no se presenta.

V.14 Consumo de potencia

El protocolo ZigBee fue diseñado con base en el estándar IEEE 802.15.4 debido a su capacidad de bajo consumo de potencia, algunas de las características de la capa física de este estándar que hacen posible el desgaste mínimo de la batería son las siguientes (Callaway, 2003):

- Señalización ortogonal multinivel.
- Reducción del consumo de potencia durante en la inicialización del transmisor, con el uso de DSSS (Direct Sequence Spread Spectrum).
- No opera en modo duplex para evitar los picos de corrientes que se generan.

En cuanto a las características de bajo consumo de potencia de la capa MAC utilizadas por ZigBee se encuentran las siguientes:

Modo de extensión de vida de la batería (BLE por sus siglas en Inglés). Debido a que uno de los desgastes de potencia principales, en redes CDMA/CA es el de mantener encendido el receptor a la espera de mensajes, el modo de trabajo BLE busca alargar la vida de las baterías tomando corriente de las mismas por periodos cortos de tiempo en lugar de tomar la corriente promedio de manera constante (Callaway, 2003). Para esto los nodos IEEE 802.15.4 están dotados con la capacidad de mantener sus receptores en modo inactivo durante un periodo determinado para después despertar y sincronizarse con su nodo padre. En el protocolo ZigBee los únicos nodos dotados de ésta capacidad son los ZED, debido a que los ZR y el ZC deben mantenerse activos como receptores para ser capaces de realizar el enrutamiento de mensajes.

Por su parte el algoritmo de enrutamiento ZigBee busca reducir la cantidad de reintentos de envío para lo cual toma en cuenta la calidad del enlace tanto como el número de saltos, en la búsqueda del mejor enlace punto a punto con el mínimo de saltos posibles (Douglas et al., 2003).

Como puede observarse, el protocolo ZigBee fue diseñado para que desde la base de las capas física y de acceso al medio contara con diferentes medios para el ahorro de energía, de igual manera el diseño general de funcionamiento del protocolo tanto en el enrutamiento como la sincronización para extensión de la

batería buscan optimizar el uso de la batería en la capa de red. Por lo demás, el consumo de potencia específico de un dispositivo dependerá en gran medida del hardware utilizado así como del comportamiento específico de la aplicación, pero puede decirse que el protocolo otorga una gran variedad de métodos y posibilidades para la implementación y el funcionamiento de aplicaciones que generen un mínimo consumo de energía.

V.15 Conclusiones

Los resultados de las pruebas permiten observar los límites de desempeño del protocolo, para algunas de las características definidas en el Capítulo II, como son: ancho de banda, eficiencia, tamaño de mensajes, redundancia, número de dispositivos, respuesta en tiempo e integridad de los datos. La cantidad de datos obtenida es considerable por lo que es necesario verificar estos valores y compararlos con los obtenidos en el Capítulo II, para protocolos cableados. Es importante notar que algunos resultados como la respuesta en tiempo, dependen en gran medida del *hardware* o el *firmware* utilizado. Sin embargo, para el caso del ancho de banda se hizo visible que la arquitectura en capas representa un retraso considerable en la generación de mensajes. Es probable que debido a la complejidad de los encabezados del protocolo y la gran cantidad de opciones que contienen las tramas de control de esos encabezados, generen una sobrecarga de trabajo que podría ser evitada para el envío de mensajes sencillos, con lo cual podría ser posible agilizar el tiempo de transmisión de mensajes.

CAPÍTULO VI

CONCLUSIONES Y APORTACIONES

En este capítulo se detallan las conclusiones a las que se llega a partir de los resultados mostrados en el Capítulo V, y el análisis de las soluciones que se realiza en el Capítulo II. Se mantiene el orden del capítulo anterior en cuanto al desarrollo de conclusiones de acuerdo a las características probadas en el protocolo, sin embargo se hace énfasis en la comparación con las redes utilizadas actualmente y los requerimientos ISA mencionados en el Capítulo II.

VI.1 Conclusiones

A continuación se presentan en resumen los valores de ancho de banda comprobados para los dispositivos ZigBee utilizados.

Tabla XIX. Ancho de Banda Útil

	Máxima Carga Útil		Mínima Carga Útil	
	Msj/s	Kbps	Msj/s	Kbps
Tx	15	13.3	40	9.4
Rx	9	8.3	9	7

Puede observarse en la Tabla XIX que el principal problema de aprovechamiento del ancho de banda está en la recepción, por lo que éste es el

límite que puede tomarse para determinar el tipo de aplicaciones en que puede ser utilizado el protocolo. Al hacer la comparación con los valores de ancho de banda de las redes cableadas, se puede considerar a ZigBee como un protocolo restringido a aplicaciones que necesiten a lo más un ancho de banda útil de 8.3 kbps, lo que lo deja en el rango de aplicaciones para interconexión de dispositivos de campo, debido a que queda dentro de los valores del protocolo AS-i mostrados en la Tabla IV.

En cuanto a la distancia máxima, como se mencionó anteriormente, depende en gran medida del tipo de dispositivos que se utilice, y debe tomarse en cuenta la posibilidad de enrutamiento de los mensajes; lo que a costa de un retraso máximo de 15 ms (Prueba 6 *Tiempo de recuperación de ruta - Redundancia*.), puede permitir ampliar la distancia de comunicación al doble.

El tamaño máximo teórico de una red ZigBee es de 65000 nodos, sin embargo deben tomarse en cuenta los problemas de ancho de banda y retrasos que puede ocasionar el crecimiento de la red, como pudo observarse en la Prueba 1 *Integridad de los datos - Estrella***.** En una red estrella de 7 nodos era posible que 6 nodos transmitieran la totalidad de sus mensajes con un periodo de 50 ms, sin embargo, la cantidad máxima que el nodo central es capaz de escuchar está alrededor de los 1650 mensajes. Por lo que puede considerarse inútil tener una red de sensores que deba mandar una cantidad mayor al nivel máximo de mensajes que pueda escuchar el nodo receptor. En conclusión, existe la posibilidad de

conectar una red tan grande como se requiera, siempre y cuando la cantidad de datos enviada no rebase las posibilidades de recepción o transmisión de los nodos.

Como también se mencionó, el tamaño de mensaje puede variar desde un mínimo de 25 bytes hasta un máximo de 128 bytes, sin embargo debe tomarse en cuenta la velocidad a la que serán transmitidos los mensajes para evitar la sobrecarga del nodo y una pérdida excesiva de información y tiempo debido a retrasos y retransmisiones. De acuerdo a los resultados de las pruebas realizadas los mensajes de tamaño mínimo, pueden ser enviados con un periodo de 40 ms como puede observarse en la Prueba 1, la Prueba 2 y la Prueba 3 del Capítulo IV. Sin embargo, cuando se utilizan mensajes de tamaño máximo, es mejor que sean enviados con un periodo mínimo de 50 ms de acuerdo a las mismas pruebas. En comparación con las redes cableadas estudiadas, ZigBee se mantiene en el rango de redes para aplicaciones de monitoreo y control de dispositivos de campo ya que puede enviar mensajes cortos. Sin embargo, para mensajes de este tipo su eficiencia disminuye en forma considerable, ya que enviar un mensaje con formato ZigBee con un solo byte de carga útil equivale a 3.8% de eficiencia. Por lo que el gasto en consumo de potencia y tiempo total de transmisión podrían resultar excesivos para aplicaciones donde el costo de diseño e instalación de una red cableada sea mínimo, ya sea por la sencillez para la conexión de los nodos, o bien un tamaño pequeño de red.

En cuanto al consumo de potencia, ZigBee propone varios métodos para el ahorro de energía, mismos que se mencionan en el capítulo anterior. En este sentido no existe ningún punto de comparación con las redes cableadas, las cuales no tienen necesidad de ahorrar energía debido a que pueden ser alimentadas a través de los mismos cables para envío de datos, o con una conexión paralela. Sin embargo puede existir un ahorro significativo en costos para la empresa que instale una red inalámbrica de sensores, debido a la inexistencia de una red paralela para alimentación de los sensores.

Al abordar el consumo de energía de las redes inalámbricas hablamos también del consumo de pilas y baterías eléctricas, el cuál representa un importante foco de contaminación, debido a que aproximadamente el 30% de sus componentes son altamente tóxicos. Por esta razón debe al menos considerarse el tema de la contaminación provocada por éstos dispositivos, sobre todo en aplicaciones donde las características propias del ambiente impiden la entrada del hombre para dar mantenimiento a las redes y realizar la recolección apropiada de las baterías. Probablemente para los tamaños de red necesitados actualmente no será requerida una gran cantidad de baterías, pero si la visión a futuro es el uso masivo de dispositivos inalámbricos, la investigación debe dirigirse también a resolver el problema de desecho de pilas o bien al uso de fuentes de energía menos tóxicas.

Debido a la falta de nodos con una mayor capacidad de transmisión, solo pudo verificarse que no existe una variación importante en el tiempo de respuesta de los dispositivos. Sin embargo en el caso de la Prueba 5. *Integridad de los datos – Multisalto* pudo observarse un retraso promedio de 17.25 ms para la retransmisión multisalto de mensajes de cualquier tamaño. Este retraso es considerable, debido que cualquier necesidad de retransmisión de mensajes para aumento de distancia de envío se verá afectado por él. En cuanto a la redundancia, debe tomarse en cuenta la posibilidad de un retraso de hasta 126 ms para la búsqueda de una nueva ruta. Debido a que las probabilidad del funcionamiento en conjunto de enrutamiento y transmisión multisalto son altas, para este tipo de aplicaciones se debe considerar el retraso mínimo como la suma de ambos, y debe aumentarse con la cantidad máxima de saltos que pueda existir. En conclusión, una red ZigBee con mayor distancia y saltos será significativamente más lenta que una red estrella sencilla. Sin embargo los tiempos de respuesta y los retrasos quedan aún dentro del rango de los milisegundos, por lo que la red ZigBee podría ser apropiada para las aplicaciones de clase 2 y 3 de la categoría de control definidas por la ISA y mostradas en la Tabla VI del Capítulo II.

En cuanto a la integridad de los datos, puede considerarse asegurada siempre y cuando el periodo de transmisión esté por encima de los 50 ms, para cualquier tamaño de mensaje y para una profundidad máxima de 2 nodos, debido a la poca capacidad del receptor. Sin embargo, conforme aumente el periodo de transmisión de los mensajes es posible aumentar el tamaño de la red sin ver

afectada la integridad de los datos. En cuanto a la distancia sólo pudo comprobarse que existe mayor pérdida de la señal entre los 15 y 20 metros para el módulo Panasonic que se utilizó en la Prueba 3, si éste se encuentra en el piso y que elevando el nodo 1 metro, es posible lograr conexiones hasta 75 m de distancia. Además de acuerdo a la Prueba 2, a costa de un retraso máximo de 17.25 ms es posible aumentar la distancia entre los nodos terminales utilizando retransmisión multisalto.

La capacidad de auto-recuperación de la red a través del enrutamiento es una de las más importantes del protocolo, ya que le otorga un grado mayor de confiabilidad a la aplicación en cuanto a la integridad de los datos. Puede además considerarse como una característica única de las redes de sensores inalámbricos, ya que las redes cableadas como ASi o CAN no tienen la capacidad de recuperar sus rutas a menos que exista una duplicación explícita de las mismas. Sin embargo, el costo en tiempo de recuperar una ruta, como se menciona anteriormente, son 126 ms para el peor caso observado y 75 ms para el mejor. Además debe tomarse en cuenta la imposibilidad de utilizar el enrutamiento para los casos en que se envían mensajes con tamaño máximo de carga útil en un periodo de transmisión menor a 20 ms.

En cuanto la capacidad de ZigBee para la implementación de diferentes tipos de topología se puede decir que ofrece una gran flexibilidad en la creación

de redes, que además incluye la ventaja de evitar el diseño de las líneas de cableado para lograr la configuración deseada.

Aunque el método de acceso es algo independiente del protocolo ZigBee, debe tomarse en cuenta que puede considerarse lento e ineficiente al compararlo con los de las redes cableadas estudiadas en el Capítulo II. Sin embargo, debido a las restricciones ya mencionadas en tamaño de red y periodo de transmisión, es probable que los problemas de *trashing* (característicos de CDMA) por colisiones o retransmisiones no sean frecuentes. Además como se menciona en el capítulo anterior, el diseño de la red debe tomar en cuenta los problemas del nodo escondido y el nodo expuesto que el protocolo hereda del método de acceso, para así poder utilizarlo apropiadamente.

Dos características que se encuentran sumamente ligadas son el soporte y la interoperabilidad con otros protocolos. A diferencia de otras redes de sensores, cableadas e inalámbricas, ZigBee cuenta con el soporte de una asociación de empresas grande y que continúa en crecimiento. Además, cada día existe un interés mayor por el mismo, por esta misma razón ya existen empresas que intentan introducir dispositivos para la comunicación entre ZigBee y redes de sensores cableadas. En este sentido no cabe duda que ZigBee sobresale respecto al resto de los protocolos.

Para finalizar, puede definirse a ZigBee como un protocolo apropiado para aplicaciones de clase 2 a 5, de acuerdo a la clasificación ISA de aplicaciones

industriales de monitoreo y control, mostrada en el Capítulo II. Sin embargo, no se recomienda su uso en aplicaciones críticas de clase 2, debido a los tiempos de respuesta y retrasos ocasionados por enrutamiento y transmisión multisalto. Puede ser utilizado tanto en ambientes interiores o exteriores, y existe la posibilidad de sustituir redes de monitoreo de baja densidad y tiempo de respuesta mayor a 200 ms. Debe tomarse en cuenta el hecho de que el retraso principal en la recepción y transmisión de datos se encuentra en el procesamiento de los encabezados de las diferentes capas, por lo que para mejorarlos, podrían buscarse soluciones desde ángulos diferentes: por una parte optimizar el número de instrucciones utilizadas para la transferencia de los mensajes hacia la aplicación y por otra parte hacer uso de un microprocesador más rápido.

Desde un punto de vista práctico, existe una gran cantidad de comandos dentro del protocolo ZigBee que podrían no ser necesitados en aplicaciones simples como alarmas o monitoreo en general. Sin embargo debe recordarse que ZigBee no fue diseñado como un protocolo dirigido a aplicaciones industriales o médicas en forma explícita, y que la etapa de desarrollo en que se encuentra actualmente es la de automatización del hogar, con un fuerte enfoque en la interoperabilidad de los dispositivos fabricados por diferentes marcas. Por lo tanto las pruebas sobre el protocolo se concentran en la observación de tramas enviadas por el aire, y el buen funcionamiento de los comandos al interior del dispositivo. Es probable que la aparición del *Stack Profile 2*, también llamado ZigBee Pro, como un conjunto de características ampliadas de ZigBee, mejore su desempeño en

ambientes industriales. Esta expansión del protocolo busca mejorar algunas características como: escalabilidad, fragmentación de mensajes, cambio de canal en caso de interferencia, gestión de direcciones de dispositivos, localización grupal para optimización de tráfico, recolección centralizada de datos, etc. En general las mejoras realizadas están dirigidas a atacar los puntos débiles de ZigBee en redes de mayor tamaño y con funcionalidad de monitoreo. Sin embargo a partir de la implementación del protocolo, las pruebas principales estarán enfocadas en su interoperabilidad, para posteriormente verificar el desempeño de la red bajo situaciones de estrés.

Es probable que ZigBee sea el protocolo más robusto en cuanto a soporte e interoperabilidad, sin embargo es necesario tomar en cuenta que la complejidad que implica un protocolo diseñado en base a la búsqueda de interoperabilidad, podría no ser la mejor opción para un ámbito industrial cuyo mayor problema es el manejo de redes de gran tamaño y tiempos de respuesta fijos. Por otro lado mientras los tiempos de respuesta y la tasa de transferencia de datos se encuentren dentro de las posibilidades del protocolo, ZigBee puede considerarse la mejor opción para una rápida instalación, con un amplio soporte y capacidades de seguridad y redundancia altamente confiables.

VI.2 Aportaciones

La aportación principal de ésta investigación es la determinación de valores verificados de las características del protocolo ZigBee para un desempeño favorable, y a partir de éstos la recomendación de su uso en aplicaciones de las clases 3-5 definidas por ISA. También se aporta un análisis de redes cableadas y sus características para su posterior comparación con otros protocolos de sensores inalámbricos. Además se permite dar otro punto de vista a la investigación en redes inalámbricas de sensores con observaciones específicas sobre el desempeño del protocolo en situaciones de estrés, y en aplicaciones con requerimientos parecidos a las necesidades de ambientes de monitoreo y control industrial.

VI.3 Trabajo futuro.

Falta mucho trabajo concerniente a las redes inalámbricas para entornos industriales. En todo caso esta investigación abre camino para resolver nuevas interrogantes tales como:

- Búsqueda de un diseño de arquitectura más apropiado para aplicaciones industriales.
- Generación de escenarios de prueba para las aplicaciones recomendadas.

- Comparación de otros protocolos de redes inalámbricas y su clasificación de acuerdo a la ISA.
- Diseño de un protocolo basado en la obtención de tiempos de respuesta menores y mayor eficiencia.
- Comprobación del costo de seguridad.

Bibliografía

Callaway, E. 2003. Low power consumption features of the IEEE 802.15.4/ZigBee LR-WPAN standard. Florida Communication Research LabMotorola Labs.1(67): 25 p.

Castro, J., M.L Díaz. 2004. La contaminación por pilas y baterías en México, Gaceta Ecológica INE-Semarnat. 1(72): 53-74 p.

Corrigan, S. 2002. Introduction to the Controller Area Network (CAN), Texas Instruments, Application Report. SLOA101. 16p.

De Couto, D. S. J., D. Aguayo, J. Bicket, y R. Morris. 2003. A high-throughput path metric for multi-hop wireless routing, (Mobicom'03). Proceedings of the 9th annual international conference on Mobile computing and networking. California, EUA. 134-146 p.

Decotignie, J. 2005. Ethernet-based real-time and industrial communications. Proceedings of the IEEE. 93(6) 1102- 1117 p.

Federal Information Processing Standards Publication. 2001. Announcing the Advanced Encryption Standard (AES). 197: 51 p.

Felser, M. 2005. Real-time Ethernet – Industry prospective. Proceedings of the IEEE**.** **2**(93): 1118- 1129 p.

Felser, M. y T. Sauter. 2002. The Fieldbus war: history or short break between battles. Factory Communication Systems, 4th International Workshop on Volume, Vasteras, Suecia. 73-80 p.

Gladman, B. 1999. Implementation Experience with AES Candidate Algorithms. Second AES Conference. NIST. Roma, Italia. 7-14p

Hasnaoui, S. 2001. Wireless industrial networking using CAN MAC-sublayer. Industry Applications Conference, 36th IAS Annual meeting. Chicago, EUA. 2. 1303-1310 p.

ISA-SP100.11, 2006, Wireless for industrial process measurement and control. Call for Proposal. CFP. 24 p.

ISA-SP100.11, 2007, Technical requirements for time-critical securable wireless industrial field networks. 1. SP100.11 Draft. 90 p.

ISA-SP100.14, 2006, Wireless network optimazed for industrial monitoring. Call for proposal. CFP. 24 p.

Jacott, M. 2005. Pilas y baterías: tóxicos en casa Gaceta Ecológica INE-Semarnat. Greenpeace México. 8p

Kriesel, W. R., y O.W. Madelung. 1999. AS-Interface the actuator-sensor interface for automation. Suplemento de la Segunda edición. Alemania. 30 p.

ODVA, 2007, Network infrastructure for ethernet/ip: introduction and considerations. Open DeviceNet Vendor Association, Inc. Reporte Técnico. 118 p.

Poor, R. y B. Hodges. 2002. Reliable wireless networks for industrial systems. Ember Corp. Reporte Técnico. 19 p.

Rush, W. 2003. 10 emerging technologies that will change the world. technology Review's Emerging Technologies Conference at MIT. EUA.

Samson, AG. 2007. Technical information – Foundation Fieldbus. Reporte Técnico, (4): 42 p.

Sareen, G. 2003. IEEE 1394 and industrial automation: a perfect blend. Wipro Technologies Reporte Técnico. 45 p.

Siemens AG, 1999. AS-Interface - introducción y fundamentos. Manual Técnico. SIMATIC NET. Tercera edición. 43 p.

Skogholt H., M. y Stoa, S. 2006. Practical evaluation of IEEE 802.15.4 / ZigBee medical sensor networks. Tesis de maestría. Norwegian University of Science and Technology, Electronics and Telecomunications Department. 71 p.

Sun, T., L. Chan, C. C. Han, G. Yang, y M. Gerla. 2005. Measuring effective capacity of IEEE 802.15.4 beaconless mode, University of California Los Angeles, Computer Science Department. Draft. 22 p.

Tanenbaum, A. S., C. Gamage, B. Crispo. 2006. Taking sensor networks from the lab to the jungle. Computer Magazine. 39(8). 98 – 100 p.

Thomesse, J. 2005. Fieldbus technology in industrial automation. Proceedings of the IEEE. Emerging Technologies and Factory Automation, 1(19). 651-653 p.

Verhappen, I. 2002. High Speed Ethernet - The enterprise integration enabler. IEC Pros Inc. Reporte Técnico. 22 p.