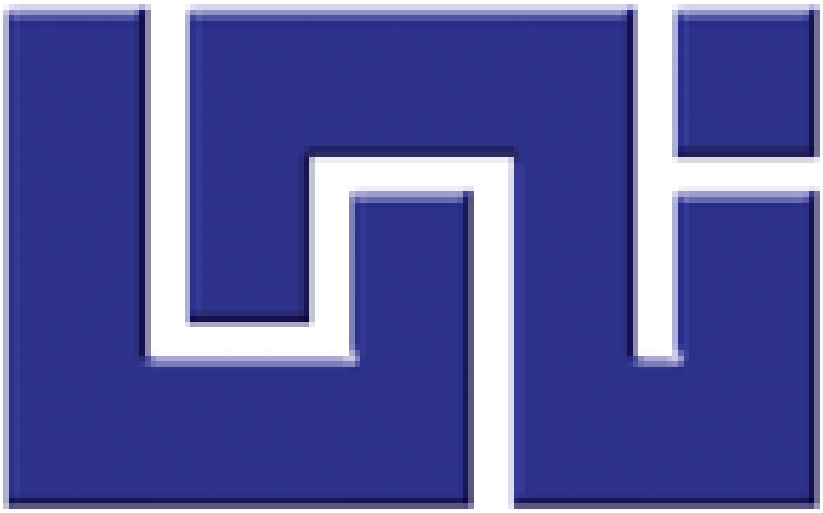
UNIVERSIDAD NACIONAL DE INGENIERÍA

(UNI)



Trabajo de Técnicas de Alta Frecuencia

TAF

Tema: Zigbee

Integrantes:

1. **Carlos Alberto Ortega Huembes. (2005-20378)**
2. **Deyanira del Socorro Roque. (2005-20900)**
3. **Leslie Eduardo Úbeda Sequeira. (2005-20917)**

Grupo: 4T2-Eo

Docente: Ing. Israel M. Zamora N.

Managua, 28 de julio de 2008

Indice

Objetivos

- Dar a conocer en qué consiste y como operan las redes Zigbee.
- Conocer sus características, ventajas y desventajas de esta tecnología.
- Determinar los parámetros a tomar en cuenta para el uso de Zigbee.
- Identificar los métodos de seguridad y comunicación que tiene esta tecnología.
- Explicar la integración de Zigbee con las tecnologías inalámbricas emergentes según los aspectos de seguridad, costos, topología, estructura, tasa de transferencia y aplicaciones.
- Comparar las redes Zigbee con las diferentes tecnologías inalámbricas.

Introducción

Las tecnologías inalámbricas han adoptado con el paso del tiempo una manera más sencilla y cómoda de utilizar toda clase de dispositivos con el fin de mejorar el confort y las comunicaciones en general. Ésta investigación aborda la tecnología inalámbrica ZigBee, basada en el estándar 802.15.4 que por su poca introducción al mercado no es muy conocida a pesar de que no es muy reciente.

ZigBee comunica una serie de dispositivos haciendo que trabajen más eficiente entre sí. Es un transmisor y un receptor que usa baja potencia para trabajar y tiene como objetivo las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías. Es ideal para conexiones con diversos tipos de topología, lo que a su vez lo hace más seguro, barato y que no haya ninguna dificultad a la hora de su construcción porque es muy sencilla.

Zigbee es la tecnología inalámbrica del futuro que no tiene competencia fuerte con las tecnologías existentes debidos a que sus aplicaciones son de automatización de edificios, hogareñas e industriales, especialmente para aplicaciones con usos de sensores.

ZigBee

C. Ortega[1], D. Roque[2] y L. Úbeda[3]

[1 2 3] Facultad de Electrotecnia y Computación, Universidad Nacional de Ingeniería (UNI)
PO Box 5595, Managua, Nicaragua
e-mail:
caoh36@yahoo.com
deya1110@hotmail.com
leslieubeda@yahoo.com

RESUMEN

ZigBee es un estándar de comunicaciones inalámbricas diseñado por la ZigBee Alliance. Es un conjunto estandarizado de soluciones que pueden ser implementadas por cualquier fabricante. ZigBee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal área Newark, WPAN) y tiene como objetivo las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

ZigBee es un sistema ideal para redes domóticas, específicamente diseñado para reemplazar la proliferación de sensores/actuadores individuales. ZigBee fue creado para cubrir la necesidad del mercado de un sistema a bajo coste, un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable.

Palabras Claves: actuadores, bajo consumo, domóticas, fiable, seguro, sensores, WPAN

Historia

El nombre "ZigBee" se deriva de los patrones erráticos comunicativos que hacen muchas abejas entre las flores durante la recogida de polen. Esto es evocador de las redes invisibles de las conexiones existentes en un entorno totalmente inalámbrico.

ZigBee (1) se ha desarrollado para satisfacer la creciente demanda de capacidad de red inalámbrica entre varios dispositivos de baja potencia. En la industria ZigBee se esta utilizando para la próxima generación de fabricación automatizada, con pequeños transmisores en cada dispositivo, lo que permite la comunicación entre dispositivos a un ordenador central.

Para llevar a cabo este sistema, un grupo de trabajo llamado Alianza ZigBee (ZigBee Alliance) formado por varias industrias, sin ánimo de lucro, la mayoría de ellas fabricantes de semiconductores, está desarrollando el estándar. La alianza de empresas está trabajando codo con codo con IEEE (2) para asegurar una integración, completa y operativa. Esta alianza en las cuales destacan empresas como Invensys, Mitsubishi, Philips y Motorota trabajan para crear un sistema estándar de comunicaciones, vía radio y bidireccional, para usarlo dentro de dispositivos de automatización hogareña (domótica), de edificios (inmótica), control industrial, periféricos de PC y sensores médicos. Los miembros de esta alianza justifican el desarrollo de este estándar para cubrir el vacío que se produce por debajo del Bluetooth (3).

Esta nueva aplicación, definida por la propia ZigBee Alliance como el nuevo estándar global para la automatización del hogar, permite que las aplicaciones domóticas(4) desarrolladas por los fabricantes sean completamente ínter operables entre sí, garantizando así al cliente final fiabilidad, control, seguridad y comodidad.

Además la ZigBee Alliance también deja disponible para su acceso la ZigBee Cluster Library, ofreciendo de este modo a los ingenieros y demás integradores, deseosos de trabajar bajo este estándar mundial idóneo para los servicios domóticos, bloques de construcción para aplicaciones con necesidades bajo el denominador común de la automatización residencial, reduciendo de este modo las labores de desarrollo y permitiendo implementaciones más precisas.

Cronología

1998. - Las redes de la familia de ZigBee se conciben, al tiempo que se hizo claro que Wi-Fi y Bluetooth no serían soluciones válidas para todos los contextos. En concreto, se observó una necesidad de redes ad hoc inalámbricas.

2003. - El estándar IEEE 802.15.4 se aprueba en mayo.

2003. - En el verano, Philips Semiconductors puso fin a su inversión en redes de mallas. Philips Lighting ha perpetuado la participación de Philips, que sigue siendo un miembro prominente de la ZigBee Alliance.

2004. - ZigBee Alliance anunció en octubre una duplicación en su número de miembros en el último año a más de 100 compañías en 22 países. En abril de 2005 había más de 150 miembros corporativos, y más de 200 en diciembre del mismo año.

2004. - Se aprueba la especificación Zigbee el 14 de diciembre.

2005. - ZigBee 2004 se puso a disposición del público sin fines comerciales el 13 de junio en San Ramón, California.

2006. – "El precio de mercado de un transceptor compatible con ZigBee se acerca al dólar y el precio de un conjunto de radio, procesador y memoria ronda los tres dólares" [(5)].

2006. - En diciembre se publicó la actual revisión de la especificación.

2007. - En Noviembre se publicó el perfil HOME AUTOMATION de la especificación.

Definición

ZigBee es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal area network, WPAN). Su objetivo son las aplicaciones para redes Wireless que requieran comunicaciones seguras y fiables con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

Estándar IEEE 802.15.4

IEEE 802.15.4 es un estándar que define el nivel físico y el control de acceso al medio de redes inalámbricas de área personal con tasas bajas de transmisión de datos (low-rate wireless personal area network, LR-WPAN). La actual revisión del estándar se aprobó en 2006. El grupo de trabajo IEEE 802.15 es el responsable de su desarrollo.
También es la base sobre la que se define la especificación de ZigBee, cuyo propósito es ofrecer una solución completa para este tipo de redes construyendo los niveles superiores de la pila de protocolos que el estándar no cubre.

Características

- ZigBee, también conocido como "HomeRF Lite", es una tecnología inalámbrica con velocidades comprendidas entre 20 kB/s y 250 kB/s.
- Los rangos de alcance son de 10 m a 75 m.
- Puede usar las bandas libres ISM [(6)] de 2,4 GHz (Mundial), 868 MHz (Europa) y 915 MHz (EEUU).
- Una red ZigBee puede estar formada por hasta 255 nodos los cuales tienen la mayor parte del tiempo el transceiver ZigBee dormido con objeto de consumir menos que otras tecnologías inalámbricas.
- Un sensor equipado con un transceiver ZigBee pueda ser alimentado con dos pilas AA durante al menos 6 meses y hasta 2 años.

- La fabricación de un transmisor ZigBee consta de menos circuitos analógicos de los que se necesitan habitualmente.
- Diferentes tipos de topologías como estrella, punto a punto, malla, árbol.
- Acceso de canal mediante CSMA/CA [(7)] (acceso múltiple por detección de portadora con evasión de colisiones).
- Escalabilidad de red -- Un mejor soporte para las redes más grandes, ofreciendo más opciones de gestión, flexibilidad y desempeño.
- Fragmentación -- Nueva capacidad para dividir mensajes más largos y permitir la interacción con otros protocolos y sistemas.
- Agilidad de frecuencia -- Redes cambian los canales en forma dinámica en caso que ocurran interferencias.
- Gestión automatizada de direcciones de dispositivos - El conjunto fue optimizado para grandes redes con gestión de red agregada y herramientas de configuración.
- Localización grupal -- Ofrece una optimización adicional de tráfico necesaria para las grandes redes.
- Puesta de servicio inalámbrico -- El conjunto fue mejorado con capacidades seguras para poner en marcha el servicio inalámbrico.
- Recolección centralizada de datos -- El conjunto fue sintonizado específicamente para optimizar el flujo de información en las grandes redes.

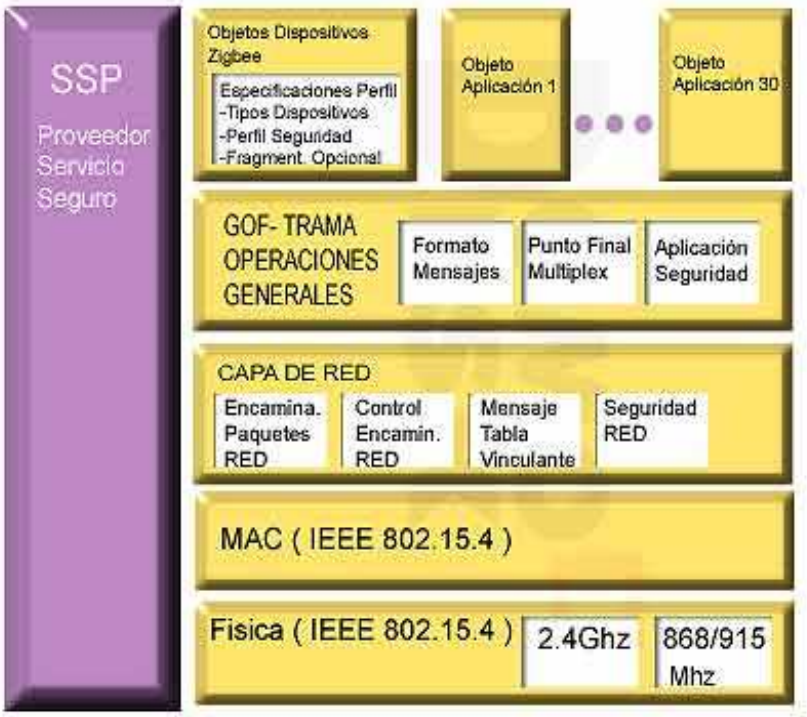
Ventajas

- Ideal para conexiones punto a punto y punto a multipunto
- Diseñado para el direccionamiento de información y el refrescamiento de la red.
- Opera en la banda libre de ISM 2.4 Ghz para conexiones inalámbricas.
- Óptimo para redes de baja tasa de transferencia de datos.
- Alojamiento de 16 bits a 64 bits de dirección extendida.
- Reduce tiempos de espera en el envío y recepción de paquetes.
- Detección de Energía (ED).
- Baja ciclo de trabajo - Proporciona larga duración de la batería.
- Soporte para múltiples topologías de red: Estática, dinámica, estrella y malla.
- Hasta 65.000 nodos en una red.
- 128-bit AES de cifrado - Provee conexiones seguras entre dispositivos.
- Son más baratos y de construcción más sencilla.

Desventajas

- La tasa de transferencia es muy baja.
- Solo manipula textos pequeños comparados con otras tecnologías.
- Zigbee trabaja de manera que no puede ser compatible con bluetooth en todos sus aspectos porque no llegan a tener las mismas tasas de transferencia, ni la misma capacidad de soporte para nodos.
- Tiene menor cobertura porque pertenece a redes inalámbricas de tipo WPAN.

Estructura



Siguiendo el estándar del modelo de referencia OSI [8] (Open Systems Interconnection), en el gráfico, aparece la estructura de la arquitectura en capas. Las primeras dos capas, la física y la de acceso al medio MAC [9], son definidas por el estándar IEEE 802.15.4. Las capas superiores son definidas por la Alianza ZigBee y corresponden a las capas de red y de aplicación las cuales contienen los perfiles del uso, ajustes de la seguridad y la mensajería.

Los cometidos principales de la capa de red son permitir el correcto uso del subnivel MAC y ofrecer un interfaz adecuado para su uso por parte del nivel inmediatamente superior. Sus capacidades, incluyendo el ruteo, son las típicas de un nivel de red clásico.

Por una parte, la entidad de datos crea y gestiona las unidades de datos del nivel de red a partir del payload del nivel de aplicación y realiza el ruteo en base a la topología de la red en la que el dispositivo se encuentra. Por otra, las funciones de control del nivel controlan la configuración de nuevos dispositivos y el establecimiento de nuevas redes; puede decidir si un dispositivo colindante pertenece a la red e identifica nuevos routers y vecinos. El control puede detectar así mismo la presencia de receptores, lo que posibilita la comunicación directa y la sincronización a nivel MAC.

La trama general de operaciones (GOF) es una capa que existe entre la de aplicaciones y el resto de capas. La GOF suele cubrir varios elementos que son comunes a todos los dispositivos, como el subdireccionamiento, los modos de direccionamientos y la descripción de dispositivos, como el tipo de dispositivo, potencia, modos de dormir y coordinadores de cada uno. Utilizando un modelo, la GOF especifica métodos, eventos, y formatos de datos que son utilizados para constituir comandos y las respuestas a los mismos.

La capa de aplicación es el más alto definido por la especificación y, por tanto, la interfaz efectiva entre el nodo ZigBee y sus usuarios. En él se ubican la mayor parte de los componentes definidos por la especificación: tanto los objetos de dispositivo ZigBee (ZigBee device objects, ZDO) como sus procedimientos de control como los objetos de aplicación que se encuentran aquí.

Tipos de Dispositivos

Se definen tres tipos distintos de dispositivo ZigBee según su papel en la red:

Coordinador ZigBee (ZigBee Coordinator, ZC): El tipo de dispositivo más completo. Debe existir uno por red. Sus funciones son las de encargarse de controlar la red y los caminos que deben seguir los dispositivos para conectarse entre ellos, requiere memoria y capacidad de computación.

Router ZigBee (ZigBee Router, ZR): Interconecta dispositivos separados en la topología de la red, además de ofrecer un nivel de aplicación para la ejecución de código de usuario.

Dispositivo final (ZigBee End Device, ZED): Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o un router), pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías. Un ZED tiene requerimientos mínimos de memoria y es por tanto significativamente más barato.

Funcionalidad

Basándose en su funcionalidad, puede plantearse una segunda clasificación:

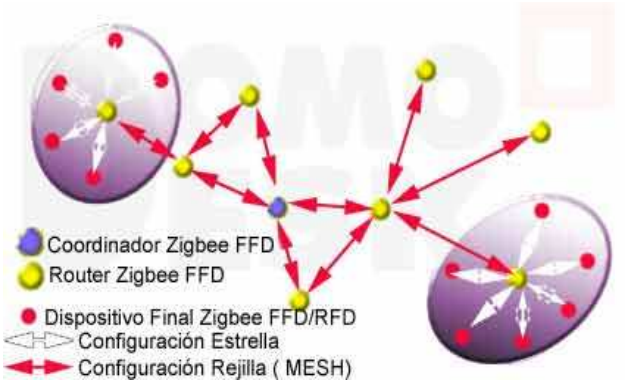
Dispositivo de funcionalidad completa (FFD): También conocidos como nodo activo. Es capaz de recibir mensajes en formato 802.15.4. Gracias a la memoria adicional y a la capacidad de computar, puede funcionar como Coordinador o Router ZigBee, o puede ser usado en dispositivos de red que actúen de interfaces con los usuarios.

Dispositivo de funcionalidad reducida (RFD): También conocido como nodo pasivo. Tiene capacidad y funcionalidad limitadas con el objetivo de conseguir un bajo coste y una gran simplicidad. Básicamente, son los sensores/actuadores de la red.

Un nodo ZigBee (tanto activo como pasivo) reduce su consumo gracias a que puede permanecer dormido la mayor parte del tiempo (incluso muchos días seguidos). Cuando se requiere su uso, el nodo ZigBee es capaz de despertar en un tiempo ínfimo, para volverse a dormir cuando deje de ser requerido. Un nodo cualquiera despierta en aproximadamente 15 ms. Además de este tiempo, se muestran otras medidas de tiempo de funciones comunes:

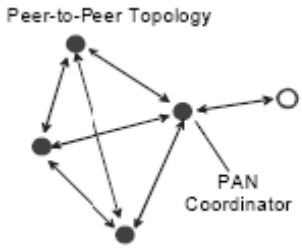
- Nueva enumeración de los nodos esclavo (por parte del coordinador): aproximadamente 30 ms.
- Acceso al canal entre un nodo activo y uno pasivo: aproximadamente 15 ms.

Topología

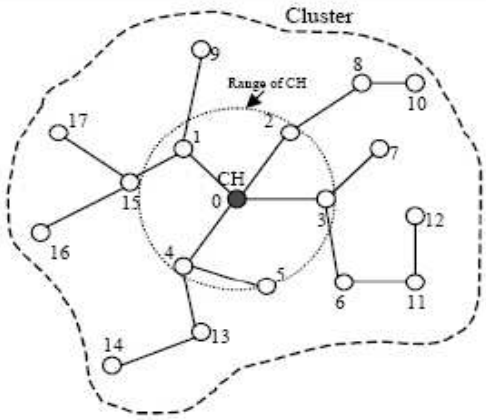


La capa de red soporta múltiples configuraciones de red incluyendo estrella, árbol, punto a punto y rejilla (malla).
En la configuración en estrella, uno de los dispositivos tipo FFD asume el rol de coordinador de red y es responsable de inicializar y mantener los dispositivos en la red. Todos los demás dispositivos zigbee, conocidos con el nombre de dispositivos finales, hablan directamente con el coordinador.

En la configuración de rejilla, el coordinador ZigBee es responsable de inicializar la red y de elegir los parámetros de la red, pero la red puede ser ampliada a través del uso de routers ZigBee. El algoritmo de encaminamiento utiliza un protocolo de pregunta-respuesta (request-response) para eliminar las rutas que no sean óptimas, La red final puede tener hasta 254 nodos. Utilizando el direccionamiento local, se puede configurar una red de más de 65000 nodos (2^{16}).



Para la topología punto a punto, existe un solo FFD Coordinador. A diferencia con la topología estrella, cualquier dispositivo puede comunicarse con otro siempre y cuando estén en el mismo rango de alcance circundante. Las aplicaciones orientadas para el monitoreo y control de procesos industriales, redes de sensores inalámbricos, entre otros, son ampliamente usados por estas redes. Proveen confiabilidad en el enrutamiento de datos (multipath routing).



La topología de árbol es un caso especial de topología de conexión punto a punto, en la cual muchos dispositivos son FFDs y los RFD pueden conectarse como un nodo único al final de la red. Cualquiera de los FFDs restantes pueden actuar como coordinadores y proveer servicios de sincronización hacia otros dispositivos o coordinadores.

Tipos de Trafico de Datos

ZigBee/IEEE 802.15.4 dirige tres tipos de tráfico típicos:

1. **Cuando el dato es periódico:** La aplicación dicta la proporción, el sensor se activa, chequea los datos y luego desactiva.

2. **Cuando el dato es intermitente:** La aplicación, u otro estímulo, determina la proporción, como en el caso de los detectores de humo. El dispositivo necesita sólo conectarse a la red cuando la comunicación se hace necesaria. Este tipo habilita el ahorro óptimo en la energía.

3. **Cuando el dato es repetitivo:** La proporción es a priori fija. Dependiendo de las hendeduras de tiempo repartidas, los dispositivos operan para las duraciones fijas.

Estrategias de conexión de los dispositivos en una red Zigbee

Las redes ZigBee han sido diseñadas para conservar la potencia en los nodos esclavos. De esta forma se consigue el bajo consumo de potencia. La estrategia consiste en que, durante mucho tiempo, un dispositivo esclavo está en modo dormido, de tal forma que solo se despierta por una fracción de segundo para confirmar que está vivo en la red de dispositivos de la que forma parte. Esta transición del modo dormido al modo despierto (modo en el que

realmente transmite), dura unos 15ms, y la enumeración de "esclavos" dura alrededor de 30ms.

En las redes Zigbee, se pueden usar dos tipos de entornos o sistemas:

Con balizas

Es un mecanismo de control del consumo de potencia en la red. Permite a todos los dispositivos saber cuándo pueden transmitir. En este modelo, los dos caminos de la red tienen un distribuidor que se encarga de controlar el canal y dirigir las transmisiones. Las balizas que dan nombre a este tipo de entorno, se usan para poder sincronizar todos los dispositivos que conforman la red, identificando la red domótica, y describiendo la estructura de la "supertrama". Los intervalos de las balizas son asignados por el coordinador de red y pueden variar desde los 15ms hasta los 4 minutos.

Este modo es más recomendable cuando el coordinador de red trabaja con una batería. Los dispositivos que conforman la red, escuchan a dicho coordinador durante el "balizamiento" (envío de mensajes a todos los dispositivos -broadcast-, entre 0,015 y 252 segundos). Un dispositivo que quiera intervenir, lo primero que tendrá que hacer es registrarse para el coordinador, y es entonces cuando mira si hay mensajes para el. En el caso de que no haya mensajes, este dispositivo vuelve a "dormir", y se despierta de acuerdo a un horario que ha establecido previamente el coordinador. En cuanto el coordinador termina el "balizamiento", vuelve a "dormirse".

Sin balizas

Se usa el acceso múltiple al sistema Zigbee en una red punto a punto cercano. En este tipo, cada dispositivo es autónomo, pudiendo iniciar una conversación, en la cual los otros pueden interferir. A veces, puede ocurrir que el dispositivo destino puede no oír la petición, o que el canal esté ocupado.

Este sistema se usa típicamente en los sistemas de seguridad, en los cuales sus dispositivos (sensores, detectores de movimiento o de rotura de cristales), duermen prácticamente todo el tiempo (el 99,999%). Para que se les tenga en cuenta, estos elementos se "despiertan" de forma regular para anunciar que siguen en la red. Cuando se produce un evento (en el sistema será cuando se detecta algo), el sensor "despierta" instantáneamente y transmite la alarma correspondiente. Es en ese momento cuando el

coordinador de red, recibe el mensaje enviado por el sensor, y activa la alarma correspondiente. En este caso, el coordinador de red se alimenta de la red principal durante todo el tiempo.

Comunicación y descubrimiento de dispositivos.

Para que los dispositivos que forman una aplicación puedan comunicarse, deben utilizar un protocolo de aplicación compartido. Estas convenciones se agrupan en perfiles. Las decisiones de asociación se deciden en base a la coincidencia entre identificadores de clusters de entrada y salida, que son únicos en el contexto de un perfil dado y se asocian a un flujo de datos de entrada o salida en un dispositivo; las tablas de asociaciones mantienen los pares de identificadores fuente y destino.

En base a la información disponible, el descubrimiento de dispositivos puede adecuarse utilizando varios métodos distintos. Si se conoce la dirección de red, se pide la dirección IEEE utilizando unicast [(10)]. Sino es así, se pide por broadcast [(11)], y la dirección IEEE forma parte de la respuesta. Los dispositivos hoja (end devices) responden con la dirección propia solicitada, mientras que routers y coordinadores envían también las direcciones de todos los dispositivos asociados a ellos.

Este protocolo extendido permite indagar acerca de dispositivos dentro de una red y sus servicios ofrecidos a nodos externos a la misma. Los endpoints pueden informar acerca de estos servicios cuando el protocolo de descubrimiento dirige mensajes a ellos. También pueden utilizarse servicios de emparejamiento oferta-demanda.

Los identificadores de cluster favorecen la asociación entre entidades complementarias por medio de tablas de asociación, mantenidas en los coordinadores ZigBee ya que estas tablas siempre han de estar disponibles en una red (los coordinadores son, de entre todos los nodos, los que con mayor seguridad dispondrán de una alimentación continua). Los backups a estas tablas, de ser necesarios para la aplicación, han de realizarse en niveles superiores. Por otra parte, el establecimiento de asociaciones necesita que se haya formado un enlace de comunicación; tras ello, se decide si adjuntar un nuevo nodo a la red en base a la aplicación y las políticas de seguridad.

Nada más establecerse la asociación pueden iniciarse las comunicaciones. El direccionamiento directo utiliza la dirección de radio y el número de endpoint; por su parte,

el indirecto necesita toda la información relevante (dirección, endpoint, cluster y atributo) y la envía al coordinador de la red, que mantiene esta información por él y traduce sus peticiones de comunicación. Este direccionamiento indirecto es especialmente útil para favorecer el uso de dispositivos muy sencillos y minimizar el almacenamiento interno necesario. Además de estos dos métodos, se puede hacer broadcast a todos los endpoints de un dispositivo, y direccionamiento de grupos para comunicarse con grupos de endpoints de uno o varios dispositivos distintos.

Seguridad

La seguridad de las transmisiones y de los datos son puntos clave en la tecnología ZigBee. ZigBee utiliza el modelo de seguridad de la subcapa MAC IEEE 802.15.4, la cual especifica 4 servicios de seguridad.

Control de accesos: El dispositivo mantiene una lista de los dispositivos comprobados en la red.
Datos Encriptados: Los cuales usan una encriptación con un código de 128 bits.
Integración de tramas: Protegen los datos de ser modificados por otros.
Secuencias de refresco: Comprueban que las tramas no han sido reemplazadas por otras. El controlador de red comprueba estas tramas de refresco y su valor, para ver si son las esperadas.

Modelo básico de seguridad.

Las claves son la base de la arquitectura de seguridad y, como tal, su protección es fundamental para la integridad del sistema. Las claves nunca deben transportarse utilizando un canal inseguro, si bien existe una excepción momentánea que se da en la fase inicial de la unión de un dispositivo desconfigurado a una red. La red ZigBee debe tener particular cuidado, pues una red ad hoc [(12)] puede ser accesible físicamente a cualquier dispositivo externo y el entorno de trabajo no se puede conocer de antemano. Las aplicaciones que se ejecutan en concurrencia utilizando el mismo transceptor deben, así mismo, confiar entre sí, ya que por motivos de coste no se asume la existencia de un cortafuegos entre las distintas entidades del nivel de aplicación.

Los distintos niveles definidos dentro de la pila de protocolos no están separados criptográficamente, por lo se necesitan políticas de acceso, que se asumen correctas en su

diseño. Este modelo de confianza abierta (open trust) posibilita la compartición de claves disminuyendo el coste de forma significativa. No obstante, el nivel que genera una trama es siempre el responsable de su seguridad. Todos los datos de las tramas del nivel de red han de estar cifradas, ya que podría haber dispositivos maliciosos, de forma que el tráfico no autorizado se previene de raíz. De nuevo, la excepción es la transmisión de la clave de red a un dispositivo nuevo, lo que dota a toda la red de un nivel de seguridad único. También se posible utilizar criptografía en enlaces punto a punto.

Arquitectura de seguridad.

ZigBee utiliza claves de 128 bits en sus mecanismos de seguridad. Una clave puede asociarse a una red (utilizable por los niveles de ZigBee y el subnivel MAC) o a un enlace. Las claves de enlace se establecen en base a una clave maestra que controla la correspondencia entre claves de enlace. Como mínimo la clave maestra inicial debe obtenerse por medios seguros (transporte o preinstalación), ya que la seguridad de toda la red depende de ella en última instancia. Los distintos servicios usarán variaciones unidireccionales (one-way) de la clave de enlace para evitar riesgos de seguridad.

Es claro que la distribución de claves es una de las funciones de seguridad más importantes. Una red segura encarga a un dispositivo especial la distribución de claves: el denominado centro de confianza (trust center). En un caso ideal los dispositivos llevarán precargados de fábrica la dirección del centro de confianza y la clave maestra inicial. Si se permiten vulnerabilidades momentáneas, se puede realizar el transporte como se ha descrito. Las aplicaciones que no requieran un nivel especialmente alto de seguridad utilizarán una clave enviada por el centro de confianza a través del canal inseguro transitorio.

Por tanto, el centro de confianza controla la clave de red y la seguridad punto a punto. Un dispositivo sólo aceptará conexiones que se originen con una clave enviada por el centro de confianza, salvo en el caso de la clave maestra inicial. La arquitectura de seguridad está distribuida entre los distintos niveles de la siguiente manera:

El subnivel MAC puede llevar a cabo comunicaciones fiables de un solo salto. En general, utiliza el nivel de seguridad indicado por los niveles superiores.

El nivel de red gestiona el ruteo, procesando los mensajes recibidos y pudiendo hacer broadcast de peticiones. Las tramas salientes usarán la clave de enlace correspondiente al ruteo realizado, si está disponible; en otro caso, se usará la clave de red.

El nivel de aplicación ofrece servicios de establecimiento de claves al ZDO y las aplicaciones, y es responsable de la difusión de los cambios que se produzcan en sus dispositivos a la red. Estos cambios podrían estar provocados por los propios dispositivos (un cambio de estado sencillo) o en el centro de confianza, que puede ordenar la eliminación de un dispositivo de la red, por ejemplo. También encamina peticiones de los dispositivos al centro de seguridad y propaga a todos los dispositivos las renovaciones de la clave de red realizadas por el centro. El ZDO mantiene las políticas de seguridad del dispositivo.

Técnicas de Modulación

Zigbee opera en dos bandas de frecuencia:

- 2.4 GHz con tasa máxima de transferencia de 250 Kbps, para este caso, modula en O-QPSK (Modulación con desplazamiento de fase en cuadratura con desplazamiento temporal).

- 868-928 MHz para tasa de datos entre 20 y 40 Kbps, para este otro, modula en BPSK (Modulación con desplazamiento de fase binaria).

Modulación OQPSK (Offset Quadrature Phase Shift Keying)

La modulación OQPSK consiste en realizar una transición de fase en cada intervalo de señalización de bits, por portadora en cuadratura.

Modulación BPSK (Binary Phase Shift Keying)

En esta modulación se tiene como resultados posibles dos fases de salida para la portadora con una sola frecuencia. Una fase de salida representa un 1 lógico y la otra un 0 lógico. Conforme la señal digital de entrada cambia de estado, la fase de la portadora de salida se desplaza entre dos ángulos que están 180° fuera de fase.

- Un canal entre 868MHz y 868.6MHz, Ch1 hasta Ch10.
- Diez canales entre 902.0MHz y 928.0MHz, Ch1 hasta Ch10.
- Dieciséis canales entre 2.4GHz y 2.4835GHz, Ch11 hasta Ch26.

El estándar ZigBee especifica una sensibilidad en el receptor de -85dBm en la banda de los 2.4GHz. Y un sensibilidad de -92dBm en la banda 865/915MHz.

Aplicaciones

Los protocolos ZigBee están definidos para su uso en aplicaciones embebidas con requerimientos muy bajos de transmisión de datos y consumo energético. Se pretende su uso en aplicaciones de propósito general con características auto organizativas y bajo coste (redes en malla, en concreto). Puede utilizarse para realizar control industrial, albergar sensores empotrados, recolectar datos médicos, ejercer labores de detección de humo o intrusos o domótica. La red en su conjunto utilizará una cantidad muy pequeña de energía de forma que cada dispositivo individual pueda tener una autonomía de hasta 5 años antes de necesitar un recambio en su sistema de alimentación.

Comparación de Tecnologías Inalámbricas			
	Wi-fi	**Bluetooth**	**ZigBee**
Bandas de Frecuencias	2.4GHz	2.4GHz	2.4GHz, 868 / 915 MHz
Tamaño de Pila	~ 1Mb	~ 1Mb	~ 20kb
Tasa de Transferencia	11Mbps	1Mbps	250kbps (2.4GHz) 40kbps (915MHz) 20kbps (868MHz)
Números de Canales	11 - - 14	79	16 (2.4GHz) 10 (915MHz) 1 (868MHz)
Tipos de Datos	Digital	Digital, Audio	Digital (Texto)
Rango de Nodos Internos	100m	10m - 100m	10m - 100m
Números de Dispositivos	32	8	255 / 65535
Requisitos de Alimentación	Media - Horas de Batería	Media - Días de Batería	Muy Baja - Años de Batería
Introducción al Mercado	Alta	Media	Baja
Arquitecturas	Estrella	Estrella	Estrella, Árbol, Punto a Punto y Malla
Mejores de Aplicaciones	Edificio con Internet Adentro	Computadoras y Teléfonos	Control de Bajo Costo y Monitoreo
Consumo de Potencia	400ma transmitiendo, 20ma en reposo	40ma transmitiendo, 0.2ma en reposo	30ma transmitiendo, 3ma en reposo
Precio	Costoso	Accesible	Bajo
Complejidad	Complejo	Complejo	Simple

Futuro del Zigbee.

Se espera que los módulos ZigBee sean los transmisores inalámbricos más baratos de la historia, y además producidos de forma masiva. Tendrán un coste aproximado de alrededor de los 6 euros, y dispondrán de una antena integrada, control de frecuencia y una pequeña batería. Ofrecerán una solución tan económica porque la radio se puede fabricar con muchos menos circuitos analógicos de los que se necesitan habitualmente.

Conclusiones

Durante el desarrollo de esta investigación se ampliaron los conocimientos acerca de las tecnologías inalámbricas existentes y con mayor futuro dentro de las comunicaciones en especial Zigbee. Es interesante conocer más de cerca el tipo de aplicaciones reales a las que próximamente nos vamos a dedicar en nuestra vida laboral. Esta investigación fue dedicada a los usos más importantes y las aplicaciones recientes, por lo tanto nos pareció interesante la investigación ya que nos ayudó a comprender mejores aspectos técnicos que no sabíamos que existían de la tecnología inalámbrica Zigbee.

Zigbee a pesar que tiene muchas ventajas en sus aplicaciones no es muy utilizada debido a que no está muy introducido al mercado actual aunque ya tiene muchos años de existir, también porque no tiene compatibilidad con tecnologías actuales como bluetooth por ejemplo.

La primera impresión causo un acercamiento más profundo a éste tipo de tecnologías, fue positivo de acuerdo al objetivo marcado que era el de conocer desde este momento el tipo de redes existentes y su funcionamiento. Se puede concluir que el trabajo fue realizado sin contratiempos y se espera que en un futuro se logre aprender más a fondo cada una de las aplicaciones electrónicas citadas en el texto.

Recomendaciones

- Zigbee está diseñado específicamente para ser la solución a problemas inalámbricos siendo una unidad pequeña capaz de proveer monitoreo remoto inalámbrico a sensores y a unidades simples de entrada como controles de luces.

- ZigBee Alliance propone a Zigbee como el nuevo estándar global para la automatización del hogar, porque permite que las aplicaciones domóticas desarrolladas por los fabricantes sean completamente interoperables entre sí, garantizando así al cliente final fiabilidad, control, seguridad y comodidad.

- ZigBee es un estándar abierto, permitiendo que terceros mejoren la interoperabilidad entre dispositivos y las características generales del estándar.

- Zigbee es una tecnología WPAN que tiene la habilidad de formar una red de malla entre nodos permitiendo que el corto alcance entre nodos individuales sea expandido y multiplicado cubriendo un área mayor.

- Esta nueva aplicación fue creada para cubrir la necesidad del mercado de un sistema a bajo coste, un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable.

Referencias

(1) Marca Registrada por ZigBee Alliance.

(2) IEEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial cuyo trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales. - **http://es.wikipedia.org/wiki/Computer_Society**

(3) Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). **http://es.wikipedia.org/wiki/Bluetooth**

(4) El término domótica proviene de la unión de las palabras domus (que significa casa en latín) y tica (de automática, palabra en griego, 'que funciona por sí sola'). Es el conjunto de sistemas capaces de automatizar una vivienda, aportando servicios de gestión energética, seguridad, bienestar y comunicación, y que pueden estar integrados por medio de redes interiores y exteriores de comunicación. **http://es.wikipedia.org/wiki/Dom%C3%B3tica**

(5) Adams, Jon; Bob Heile (2005-10). Busy as a ZigBee. [IEEE]. Compare with Other Technologies. Bluetooth SIG.

(6) ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en areas industrial, científica y médica. - **http://es.wikipedia.org/wiki/Banda_ISM**

(7) Es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. En lugar de transmitir se espera un tiempo aleatorio adicional corto y si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. **http://es.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoid ance**

(8) El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO; esto es, un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

http://es.wikipedia.org/wiki/Capa_de_aplicaci%C3%B3n#Capa_de_aplicaci.C3.B3n_.28Capa_7.29

(9) Define la subcapa de control de acceso al medio según el Modelo de Referencia OSI.
http://es.wikipedia.org/w/index.php?title=Control_de_Acceso_al_Medio&redirect=no

(10) Es un envío de información desde un único emisor a un único receptor.
http://es.wikipedia.org/wiki/Unicast

(11) Broadcast, en castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.
http://es.wikipedia.org/wiki/Broadcast_(Sobre_IP)

(12) En redes de comunicación, dicha expresión hace referencia a una red (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los ordenadores están en igualdad de condiciones. Ad hoc es el modo más sencillo para el armado de una red. Sólo se necesita contar con 2 placas o tarjetas de red inalámbricas (de la misma tecnología). - **http://es.wikipedia.org/wiki/Ad_hoc**

Bibliografía (Web grafía)

ZigBee Alliance Web site

http://www.zigbee.org/en/

El Zumbido de las Abejas, ZIGBEE

http://www.osiriszig.com/content.aspx?co=15&t=21&c=2

Zigbee

http://www.casadomo.com/noticiasDetalle.aspx?c=28&id=2200

ZigBee

http://es.wikipedia.org/wiki/ZigBee

ZigBee (especificación)

http://es.wikipedia.org/wiki/ZigBee_(especificaci%C3%B3n)

Comparing WLAN and ZigBee for embedded applications

http://rfdesign.com/next_generation_wireless/who-needs-zigbee/

Architecture (Arquitectura)

http://www.tutorial-reports.com/wireless/zigbee/zigbee-architecture.php

ZigBee Characteristics (Características Zigbee)

http://www.tutorial-reports.com/wireless/zigbee/zigbee-characterstics.php

Network Model (Modelo de Red)

http://www.tutorial-reports.com/wireless/zigbee/zigbee-network-model.php

Traffic Types (Tipos de Tráfico)

http://www.tutorial-reports.com/wireless/zigbee/zigbee-traffic-types.php

ZigbeeCongresoNov2006_UFT (PDF) – Experimento Realizado

http://hispabyte.net/foro/index.php?action=dlattach;topic=19490.0;attach=578

BlueTooth_Zigbee (PDF)

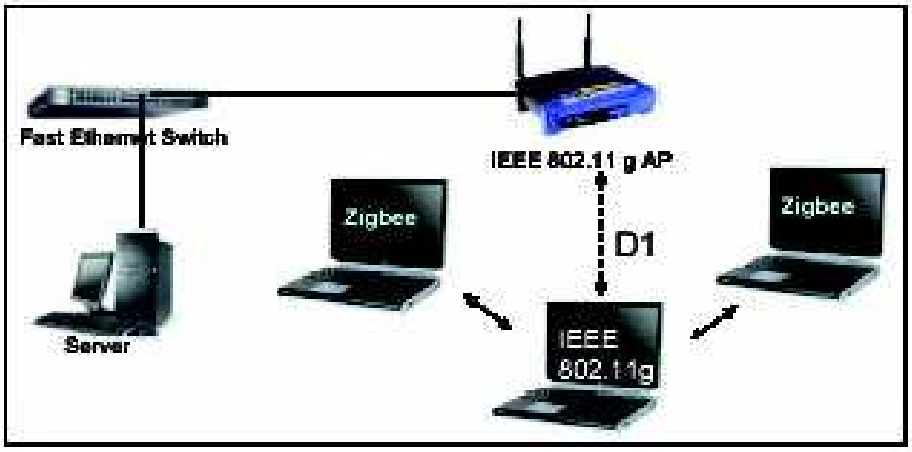
http://www.acis.org.co/memorias/JornadasTelematica/IIJNT/BlueTooth_Zigbee.pdf

Anexos

Experimento Realizado

Elementos Utilizados:

- Dispositivo Linksys IEEE 802.11g Acces Point (AP).
- Dos Laptops Dell Latitude D600 con una Maxstream XBee-PRO USB RF módems (ZigBee) usando antenas de omnidireccionales de 15cm o tarjetas interfaces Bluetooth y otra laptop similar con su respectiva tarjeta interface IEEE 802.11g



El AP y el servidor fueron conectados a un Switch Fast Ethernet, mientras la laptop con la interfaz IEEE 802.11.g se colocó en una mesa de 80cm de alto a 10.5m del AP, colocado a una altura de 2.5m en un poste.

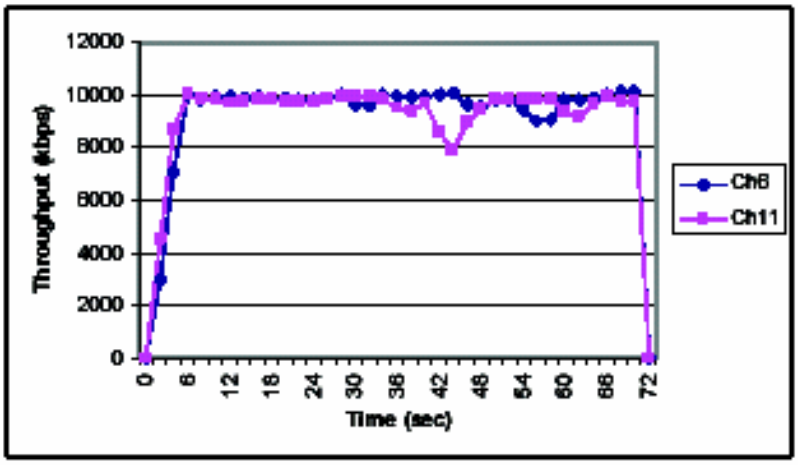
Tráfico

El tráfico fué generado usando el software “LANTrafficV2” con un packet payload de 1460 bytes y un inter-packet delay de 1ms. Para todas las pruebas 60.000 paquetes fueron transferidos entre el IEEE 802.11g cliente y el servidor (PC Server)

Se activó el modo de protección RTS/CTS Handshaking en el AP Linksys _ Cuando un dispositivo quiere comunicar datos, envía un Request to Send al nodo destino, y espera por el Clear to Send message antes de transmitir cualquier dato.

¿Para qué se utiliza? Así se evita la colisión de datos entre dispositivo ¿Desventaja? Disminuye el throughput performance (desempeño de procesamiento de datos).

.



Resultado del desempeño de procesamiento

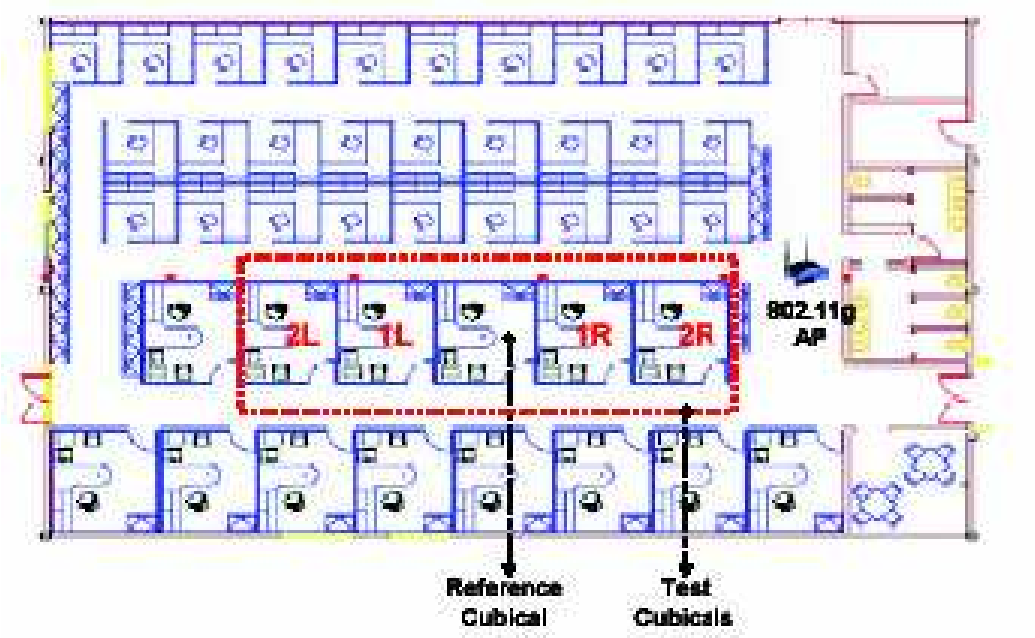
(Performance throughput of IEEE 802.11g cuando opera en los Ch16 and Ch11)

Experimento 1

IEEE 802.11g usando el Canal 11 y Zigbee usando el Canal 11

En este experimento, los dispositivos bajo el estándar IEEE 802.11g operan en el canal 11 frec 2462MHz, mientras que el canal en los módems ZigBee opera en el canal 11 bajo la frec 2405MHz.

Tanto el Cliente IEEE 802.11g y los dos dispositivos ZigBee fueron colocados como muestra la figura.



Resultado Experimento 1

IEEE 802.11g usando el Canal 11 y Zigbee usando el Canal 11

No hubo interferencia en el desempeño del cliente IEEE 802.11g ni en el dispositivo ZigBee. Luego, bajo las mismas condiciones del entorno, se hizo un reemplazo con dispositivos Bluetooth, hubo un gran efecto en el desempeño del cliente, en un promedio de caída de un 19% obteniéndose 7.9Mbps.

Experimento 2

IEEE 802.11g usando el Canal 6 y Zigbee usando el Canal 17

En este experimento, los canales de operación fueron elegidos donde el espectro iba a coincidir con cada dispositivo.
-Ch6 opera a 2437MHz - IEEE 802.11g AP
-Ch17 opera a 2435MHz - ZigBee device.

De acá se tomaron tres casos:

Caso 1: Tanto Cliente como ZigBee en el mismo cubículo. (Idem Exp 1)
Caso 2: ZigBee device colocado en cubículo R1 y otro en L1 (6m de separación entre ellos aprox.). Cliente 802.11g en el cubículo de referencia.
Caso 3: Como el caso anterior, pero colocando los ZigBee devices en R2 y L2 respectivamente (12m separación aprox.).

Resultados Experimento 2

IEEE 802.11g usando el Canal 6 y Zigbee usando el Canal 17

Casos	Porcentaje caído en IEEE 802.11g hacia Zigbee	Porcentaje caído en Zigbee hacia IEEE 802.11g
1	Insignificante	10%(de 100% a 90%)
2	Insignificante	10%(de 100% a 90%)
3	Insignificante	20%(de 83% a 65%)

No hubo cambios significativos

Resultados Experimento 2

Ahora se reemplazará los dispositivos ZigBee por Bluetooth.

Casos	Porcentaje caído en IEEE 802.11g hacia Bluetooth	Porcentaje caído en Bluetooth hacia IEEE 802.11g
1	12%(de 9.8Mbps a 8.6Mbps)	21%(de 554Kbps a 440Kbps)
2	6%(de 9.8Mbps a 9.2Mbps)	36%(de 512Kbps a 328Kbps)
3	4.6%(de 9.8Mbps a 9.35Mbps)	17%(de 365Kbps a 303Kbps)

Como era de esperarse, Bluetooth afecta enormemente el performance del IEEE 802.11g Cliente y Viceversa.
Bluetooth también se ve afectado por la presencia de IEEE 802.11g en sus proximidades de operación.

Experimento 3

Efecto en la señal Uplink desde el IEEE 802.11g AP hacia el IEEE 802.11g Cliente
Disponer los dispositivos ZigBee y Bluetooth en las proximidades del AP en vez del Cliente.
- De ésta manera se busca afectar el Uplink entre el WLAN AP y su Cliente.

Cliente en el cubículo de referencia, los dispositivos interferentes colocados en diversas posiciones alineados al AP en una mesa de 50cm de alto.

D2 en metros	Porcentaje caído en IEEE 802.11g hacia Zigbee	Porcentaje caído en IEEE 802.11g hacia Bluetooth
4	11%(de 9.8Mbps a 8.7Mbps)	19%(de 9.8Mbps a 7.9Mbps)
6	6%(de 8.8Mbps a 9.2Mbps)	17%(de 9.8Mbps a 8.1Mbps)
8	Insignificante	20%(9.8Mbps a 7.8Mbps)

Experimento 4

IEEE 802.11g Weak Signal

Para simular una señal débil proveniente del AP, se coloca a una distancia lejana al cliente. Colocándolo (AP) detrás de un obstáculo que disminuyó bruscamente la intensidad de la señal. El indicador del software registró un nivel de -80dBm. Los dispositivos ZigBee fueron colocados alrededor del mismo cubículo de referencia, con el AP operando en Ch6 y el ZigBee en el Ch17.

Porcentaje caído en IEEE 802.11g hacia Zigbee	**Porcentaje caído en IEEE 802.11g hacia Bluetooth**
6%(de 6.7Mbps a 6.3Mbps)	52%(de 6.7Mbps a 3.2Mbps)