Evaluación de características técnicas para la implementación de un sistema automático de trazabilidad de bienes académicos multimedia, basado en estándares inalámbricos

Raúl Martínez Rivas

Colección Trigésimo Aniversario 1984-2014
Universidad Don Bosco
Editorial Universidad Don Bosco
El Salvador, Centroamérica

Serie
Ingeniería

Colección Trigésimo Aniversario

Apartado Postal 1874, San Salvador,
El Salvador

Diseño: Melissa Beatriz Méndez Moreno

Hecho el depósito que marca la ley

ISBN 978-99923-50-54-6

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE IMAGENES

ÍNDICE DE FIGURAS

Introducción

Las redes inalámbricas han jugado un rol importante en las últimas décadas, durante ese tiempo han evolucionado a tal grado que ya no podemos prescindir de ellas. En esta tesina se evalúan dos tecnologías WiFi protocolo 802.11, diseñada para la transmisión de datos, ampliamente ocupada por las instituciones educativas, empresas públicas y privadas y personas particulares.

La WiFi es tan necesaria que nuestros celulares ya se conectan a redes públicas para que estemos al tanto de las noticias más recientes, conectarse a las redes sociales, compartir videos, música.

Una segunda tecnología que se analiza en este documento es ZigBee protocolo 802.15.4, diseñada para la domótica o seguridad de pequeños establecimientos con bajo costo en consumo energético. Para distancias cortas, pero también hay tecnologías para distancias amplias, como es el caso que se estudia en el documento.

El trabajo se centra en el monitoreo de los bienes móviles con los que cuenta la universidad, dichos bienes son: laptops, retroproyectores, radio grabadoras, televisores y cañones. Estos equipos son una gran inversión para la Universidad y por ello se deben resguardar, tomando en consideración que han sido adquiridos a lo largo de los años de existencia de la Universidad.

Para mantener un control efectivo, se propone utilizar RFID, una tecnología de radio frecuencia que puede trabajar con WiFi como transportadora de su trama y con ello mantener un monitoreo de los bienes móviles, es tan amplio que se puede reorientar para otro tipo de trabajo de control.

Marco Teórico

RFID (siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (automatic identification, o identificación automática).

Las etiquetas RFID son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor.

¿Cómo funciona?
Todo sistema RFID se compone de un interrogador o sistema de base que lee y escribe datos en los dispositivos y un transponder o transmisor que responde al interrogador.

1. El interrogador genera un campo de radiofrecuencia, normalmente conmutando una bobina a alta frecuencia. Las frecuencias usuales van desde 125 Khz hasta la banda ISM de 2.4 Ghz, incluso más.
2. El campo de radiofrecuencia genera una corriente eléctrica sobre la bobina de recepción del dispositivo. Esta señal es rectificada y de esta manera se alimenta el circuito.
3. Cuando la alimentación llega a ser suficiente el circuito transmite sus datos.
4. El interrogador detecta los datos transmitidos, por la tarjeta como una perturbación del propio nivel de la señal.

Protocolos y opciones
Normalmente, el sistema de modulación usado es modulación de amplitud (AM) con codificación tipo Manchester NRZ.

Para conseguir mayor alcance y más inmunidad al ruido eléctrico se utilizan sistemas más sofisticados. En algunos casos, se divide la frecuencia del reloj de recepción.

La mayor parte de los sistemas tienen una memoria EEPROM donde se almacenan datos. En algunos casos llevan datos grabados de fábrica y en otros también hay datos que puede grabar el usuario.

Algunos sistemas utilizan encriptación de clave pública para conseguir mayor seguridad ante posibles escuchas maliciosas.

Por otro lado, podemos encontrar sistemas anticolisión que permiten leer varias tarjetas al mismo tiempo. En caso de que varias tarjetas estén en el rango de alcance del interrogador y dos o más quieran transmitir al mismo tiempo, se produce una colisión. El interrogador detecta la colisión y manda parar la transmisión de las tarjetas durante un tiempo. Después irán respondiendo cada una por separado por medio de un algoritmo bastante complejo.

En la actualidad, los sistemas son utilizados para monitorear productos que se encuentran en un almacén o son enviados a otros sitios distantes, esto es seguridad a los bienes de una empresa o compañía. Otro aspecto de utilización es el médico, ya que se puede monitorear un paciente en estado delicado. Teniendo para ello el expediente a la mano esto lo logramos por medio de un lector especial.

Como vemos, los activos son la parte importante de una empresa, en una institución educativa, esto no es la excepción, contamos con retroproyectores, cañones, radiograbadoras, televisores y otros equipos delicados que necesitan ser monitoreados, además se puede tener un control de los vehículos propios de la institución, este tipo de control es muy adecuado, se puede verificar su ubicación y movimiento dentro de la universidad e inclusive la ciudadela, en cada caceta tendría que haber un sistema que no permita la salida de los vehículos con un control especial.

Esto se puede llevar más allá, desde un control de vehículos particulares que ingresan a la universidad hasta los vehículos de los estudiantes y docentes, de igual manera se tendría el control de los estudiantes que ingresan, desde el momento que pase una puerta ya se estaría observando el ingreso, si dado caso ingresará un extraño o visitante no habría señal en el sistema de monitoreo, por lo cual se podría retener y preguntar el motivo de la visita.

Se podría controlar la asistencia a las clases, pero aún va más allá: controla las horas de entrada y salida del personal en general que labora en la universidad, ingreso a la misma, he inicio de su clase con su respectiva finalización.

Problemática a resolver

En la Universidad Don Bosco, se cuenta con diferentes equipos para el buen desarrollo de las actividades académicas, e inclusive las actividades en las que participan las autoridades de la Universidad, tales como: cañones, retroproyectores, televisores, radio grabadoras, laptops. Esto activos tienen un costo monetario y son ampliamente utilizados, por ser de tamaño pequeño, fácilmente se esconden en maletines, mochilas y baúles de vehículos.

En relación con el empleo de equipos audiovisuales por los docentes a la hora de impartir las clases se da el problema del llenado de formulario de uso de equipos a través del personal de secretaría de las respectivas escuelas. Luego, dichos equipos son llevados a las aulas por el personal de servicio responsable. Sin embargo, cuando hay varias solicitudes que hay que atender al mismo tiempo, se generan problemas tanto en la entrega como en la recepción de los equipos por diferentes circunstancias. Y esto ha sido el motivo de la perdida o extravió de tales aparatos.

Por cuyo motivo, se propone un estudio con tecnología de transmisión de datos para poder monitorear los equipos móviles, se analizará WiFi como la tecnología usada en la UDB-CS, con toda su infraestructura establecida y ZigBee, como una alternativa de comunicación, aclarando que ZigBee no está diseñado para ser usado en la comunicación a internet, más bien para el control de domótica, para estas tecnologías de comunicación se analizará equipos RFID que se podrían instalar y con ello tener un mejor control de los equipos móviles (laptops, cañones, retroproyectores, radio grabadoras).

Para lograr lo anterior, se estudiarán las redes instaladas en la UDB – CS, relación distancia de los Access Point (AP) y Decibeles dB, para así determinar la viabilidad de la propuesta.

Primera etapa.
Evaluación de características técnicas WiFi - ZigBee

1.1 WiFi con enfoque técnico basado en estándares.

EL protocolo 802.11, se halla destinado a las comunicaciones inalámbricas. Diseñado para conexión de equipos tales como computadoras, impresoras, acceso a datos y donde más ha tenido auge en el internet, se usa en áreas pequeñas, con un radio de acción de 20 metros óptimo a 200 metros con poca señal (en espacios libres) para comunicación, pero no si colocamos equipos AP[1] a distancias cortas entre uno y otro (15 a 20 metros), se cubriría mayor distancia, Este sistema inalámbrico permite que haya comunicación entre las computadoras portátiles, computadoras personales, tablet y otros medios electrónicos que usen WiFi con los servidores correspondientes tales como servidor internet, servicios de impresión, servicios de correo electrónico, cámaras web e inclusive hacer un point to point entre dos computadoras.

La Universidad Don Bosco, cuenta con múltiples redes usando tecnologías de radio frecuencia, dichas redes están distribuidas en todo el campus, por su puesto unas son abiertas y otras con seguridad. En los siguientes capítulos se analizarán con más cuidado; el protocolo IEEE 802.11b/g/n, permite que dos ordenadores conectados a una red inalámbrica intercambien datos a una velocidad de 11/54 o más Mbps[2][1].

Estos estándares nacen del protocolo IEEE 802.11[3][2].

Uno de los protocolo más utilizados para la comunicación vía internet en equipos tales como laptop, impresoras tablet e inclusive teléfonos celulares, en la industria para la transferencia de datos vía internet es el 802.11g, Ratificado en el año 2003. En la tabla 1, se analiza el protocolo mencionado y su familia hasta los más recientes aprobados en el año 2012.

1. AP: Access Point.
2. Mbps: Mega bits por segundo, Soyer, Laurence, Wi-Fi: Instalar una red inalámbrica en casa, Ediciones ENI Po Ferrocarriles Catalanes, 97-117, 2gndo. pl.of.18 08940-Cornella de Llobregat Barcelona – España. Agosto 2005
3. IEEE 802.11 Estándar que fue ratificado en julio de 1997 funciona en la banda de 2,4GHz con velocidad de transmisión máxima de 2Mbps, ha sido el más utilizado en las redes WLAN, F. Andreu, WLAN Fundamentos y aplicaciones de seguridad, Marcombo, S.A de C.V 2006, Página 22.

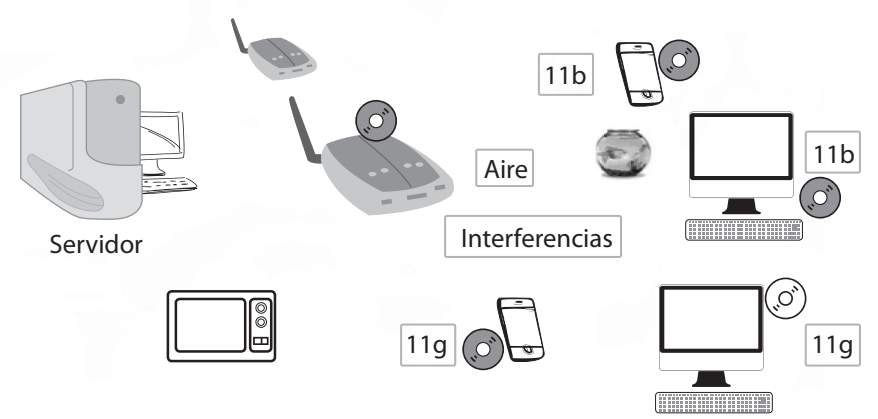


Figura 1. De conexión de una red WiFi que involucra diferentes componentes electrónicos

En la Universidad Don Bosco, como en cualquier lugar de trabajo existente, hay oficinas que cuentan con equipos eléctricos y electrónicos que pueden interrumpir la señal de la red inalámbrica WiFi. En el diagrama se muestra los diferentes equipos que pueden conectarse en la WiFi, pero igual aquellos que pueden producir interferencia en la señal, un microondas, que esté cerca de la base de antena WiFi o del ordenador puede interrumpir la señal, un buen número de celulares trabaja en la banda de 2.4 Ghz, esto también interrumpe el buen funcionamiento del sistema de red, ya que el canal de transmisión es ocupado por estos componentes. No solo esto interfiere una señal, para ellos explicamos los siguientes puntos:

La siguiente información es tomada de
http://support.apple.com/kb/HT1365?viewlocale=es_ES&locale=es_ES

Efectos de las interferencias

- Disminución del alcance inalámbrico entre dispositivos
- Disminución de la transferencia de datos través de una red Wi-Fi
- Pérdida completa o intermitente de la conexión inalámbrica
- Dificultades para conectar los dispositivos durante la fase de detección de dispositivos Bluetooth

Fuentes de interferencias

- Hornos microondas: Utilizar tu horno microondas cerca del ordenador, dispositivo Bluetooth o estación base Wi-Fi puede producir interferencias.

- Servicio por satélite directo (DSS): El cable y los conectores coaxiales utilizados con algunos tipos de antenas parabólicas podrían producir interferencias. Comprueba que el cable no esté dañado y hazte con cables nuevos si sospechas que hay una fuga de RF.
- Ciertas fuentes eléctricas externas, como líneas de alta tensión, vías de tren electrificado y centrales energéticas.
- Teléfonos a 2,4 o 5 GHz: Un teléfono inalámbrico que funcione en este rango de frecuencias podría provocar interferencias con los dispositivos y redes inalámbricos encendidos.
- Emisores de vídeo (transmisores/receptores) que funcionen en las frecuencias de 2,4 o 5 GHz.
- Altavoces inalámbricos que funcionen en las bandas de 2,4 o 5 GHz.
- Algunos monitores externos y pantallas LCD: Puede que algunas pantallas emitan interferencias armónicas, especialmente en las bandas de 2,4 GHz de ancho de banda entre los canales 11 y 14. Puede que esta interferencia llegue a su extremo si tienes un ordenador portátil con la tapa cerrada y un monitor externo conectado al mismo. Intenta cambiar el punto de acceso para utilizar el canal de 5 GHz o inferior a 2,4 GHz.
- Cualquier otro dispositivo inalámbrico que funcione en las frecuencias de 2,4 o 5 GHz (microondas, cámaras, intercomunicadores para bebés, dispositivos inalámbricos cercanos).
- Nota: Algunos dispositivos podrían no mencionar explícitamente que operan en frecuencias de 2,4 o 5 GHz. La documentación del producto debería indicar qué bandas utiliza el dispositivo. Estos dispositivos suelen denominarse “de banda de frecuencia dual”, “Wi-Fi” o “inalámbricos”.

Entorno del hogar y de la oficina

Si es posible, evitar barreras inalámbricas o cambiar la ubicación de los dispositivos Wi-Fi o Bluetooth para despejar la trayectoria de la señal. La ubicación del dispositivo dentro de un edificio y los materiales de construcción utilizados pueden afectar a la conexión Wi-Fi y Bluetooth. En la tabla que aparece a continuación se muestran los materiales más comunes que impiden las conexiones y la posibilidad de que ocasionen interferencias.

Tabla 0. Obstrucciones absorbentes y reflectantes de radiofrecuencia (RF)

Tipo de barrera	Potencial de interferencia
Madera	Bajo
Material sintético	Bajo
Cristal	Bajo
Agua	Medio
Ladrillos	Medio
Mármol	Medio
Escayola	Alta
Hormigón	Alta
Cristal blindado	Alta
Metal	Muy alto

Cómo reducir los efectos de las interferencias provocadas por otros dispositivos inalámbricos

A fin de minimizar las interferencias entre tus dispositivos Wi-Fi y Bluetooth, se recomienda:

1. Cambiar los canales de red inalámbrica. Para las estaciones base Wi-Fi, restablecer la estación base y esta intentará utilizar los canales de 2,4 y 5 GHz que tienen menor grado de interferencias cuando se inicie de nuevo.
2. Conectarse a una red inalámbrica de 5 GHz (si es posible).
3. Reducir el número de dispositivos Bluetooth inalámbricos activos que tengas conectados al ordenador o que estén funcionando en la cercanía.

Si el rendimiento en la red inalámbrica no es óptimo por culpa de las interferencias provocadas por otros dispositivos inalámbricos, se deberá tomar las medidas adecuadas para ello, alejar la base AP de los sitios excesivamente húmedos, hornos microondas colocarlos en sitios donde no hayan obstáculos excesivos.

En la UDB-CS, ya existe una infraestructura instalada y si los equipos conectados fueron bien seleccionados para los diferentes ambientes no debería haber problema alguno, pero la realidad dicta lo contrario, hay baja señal en puntos específicos, esto se estudiará más adelante.

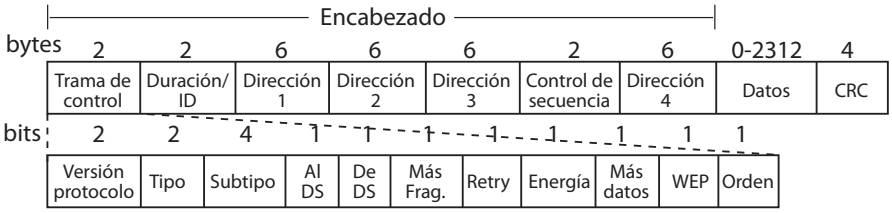


Figura 2. Trama del protocolo 802.11

Tabla 1. Descripción general de las capas físicas 802,11[4][3]

	IEEE802.11	IEEE802.11b	IEEE802.11a	IEEE802.11g	IEEE802.11n	IEEE802.11ac
Fecha	1997	1999	2000	2003	2012	2012
Banda	2.4GHz	2.4GHz	5.8GHz	2.4GHz	El estándar 802.11n existe tanto en la banda de 2.4 GHz: así como en la de 5 GHz: le permite a 802.11n cambiar dinámicamente el canal de operación de 40 MHz a 20 MHz mientras se comunica con una antena WiFi 802.11 a/b/g o un dispositivo 802.11n, lo cual se traduce en compatibilidad retroactiva a 802.11 a/b/g.	El estándar consiste en mejorar las tasas de transferencia hasta 1 Gbit/s dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz (40 Mhz en las redes 802.11n), hasta 8 flujos MIMO y modulación de alta densidad (256 QAM)
Velocidad De Transmisión	1,2MBps	1,2,5.5 y 11 MBps	6,9, 12, 18,24,36, 48, 54 MBps	1,2, 5.5,6,9, 11,12,18, 24,36,48,54, MBps	13.5,27,40.5,54,81,10 8,121.5,135 MBps	alcanza nada menos que 1.5 GBps
Modulación	DHSS,FHSS	DHSS	OFDM	OFDM	OFDM (Multiplexaje por División de Frecuencias Ortogonales) nueva y más eficiente que provee anchos de banda más amplios y mayores velocidades de datos.	OFDM
Compatibilidad		IEEE802.11	No compatible Con ningún Otro estándar	IEEE802.11 Y IEEE802.11B	compatibilidad retroactiva a 802.11 a/b/g	compatibilidad retroactiva a 802.11 a/b/g

4. WLAN, F. Andreu, WLAN Fundamentos y aplicaciones de seguridad, Marcombo, S.A de C.V, 2006, Pagina 23.

La tabla 1, da una visión general de las características de la familia 802.11, analizar la velocidad de transmisión en valores de Mega bite por segundo **"MBps"**,

La distancia mínima que cubre es de 20 metros óptima hasta una máxima de 200 metros en señal débil, **considerando otros factores que pueden atenuar la señal de los AP, están las paredes de los edificios, los árboles y quizá otros equipos de radio frecuencia que no hayan sido detectados.**

1.2 Zigbee enfoque técnico

El estándar IEEE 802.15.4 conocido como ZIGBEE, con su diferente familia está diseñado para suministrar conectividad a distancias relativamente cortas del orden 10 metros y cubrir distancias de 1600 metros máximos, está orientado para trabajar en bajo consumo, se presta su trabajo para redes inalámbricas de área personal[5]. Está hecho para comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías. Opera en el ancho de banda 2.4Ghz,

La utilidad más expandida en "DOMÓTICA", permite un ancho de banda pequeño al momento de trabajar en la tabla 2 se detallan las características entre dos tecnologías de comunicación (ZigBee y WiFi).

Un sistema ZigBee puede estar formado por 255 nodos los cuales tienen la mayor parte del tiempo el transiver ZigBee dormido con el objeto de consumir menos energía que otras tecnologías inalámbricas. Otra ventaja es que se pueden alimentar con baterías AA, que duran de 6 meses a 2 años.

Trabaja en frecuencias de 20Kbs y 250 Kbs, rango de 10mts a 75mts. Usa las bandas libres ISM de 2.6 GHz, 868 Mhz para Europa y 915 Mhz para Estados Unidos.

El ZigBee permite un consumo de potencia extremadamente bajo

- La posibilidad de estar dormidos durante grandes periodos de tiempo
- su sencillez
- su bajo costo

Esto hace que sea muy utilizado en empresas e instituciones alrededor del mundo para tener un control efectivo de personal a instalaciones de acceso restringido, control de humedad, control de humo y el control remoto de equipos electrónicos.

5. Wireless personal area network, WPAN, http://es.wikipedia.org/wiki/ZigBee, Página 1.

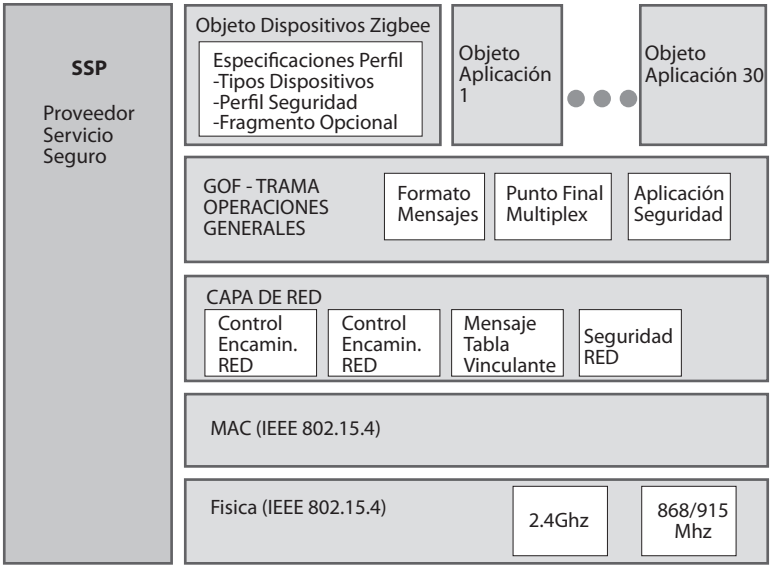


Figura 3. Arquitectura de ZigBee

Dicha arquitectura muestra la construcción interna del Zigbee.

Características de las redes/dispositivos ZigBee serían las siguientes[6]:

- Protocolo asíncrono, half duplex y estandarizado, permitiendo a productos de distintos fabricantes trabajar juntos.

- Se pueden formar redes que contengan desde dos dispositivos hasta cientos de ellos.

- Los dispositivos de estas redes pueden funcionar en un modo de bajo consumo, lo que supone años de duración de sus baterías.

- Opera en la frecuencia de 2.4 GHz (16 canales) y también en las frecuencias de 868 MHz y 915 MHz.

- Es un protocolo seguro ya que se puede implementar encriptación y autentificación.

6 .http://webpersonal.uma.es/~ECASILARI/Docencia/Memorias_Presentaciones_PFC/34Memoria_PFC.pdf

Automatización industrial. Para identificar piezas es necesario agregar alguna marca que dé alguna información[7].

Actualmente, se usan etiquetas de códigos de barra e identificadores de radiofrecuencia de tipo pasivo (passive RFID Radio Frequency Identification). Estas, son marcas (tags) formadas por un circuito integrado de memoria que cuando se acercan a un campo electromagnético de determinada frecuencia, se pueden leer y grabar. El inconveniente mayor es que solo trabajan a pocos centímetros del lector. Usando ZigBee es posible construir marcas activas (active RFID) que se lean a mayor distancia y además usarse para brindar información indirecta sobre su localización usando tres o más nodos ZigBee de ubicación conocida.

En este párrafo podemos comprobar que la tecnología ZigBee soporta a RFID para transportar traza de movilidad de equipos, de esta misma forma se puede usar para controlar lo que se ofrece en esta tesis.

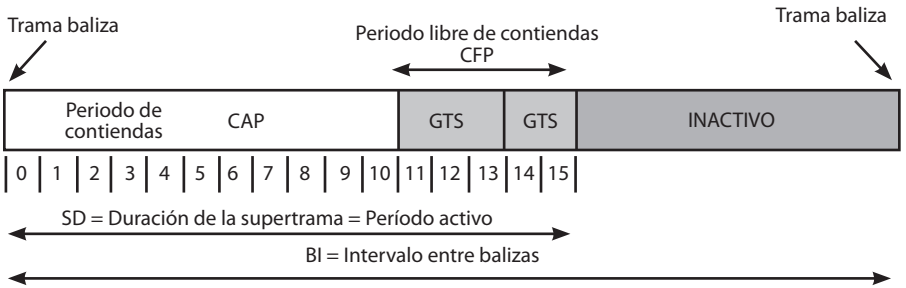


Figura 4. Presentamos una Trama Zigbee.

7. http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Dignanni_Jorge_Pablo.pdf(En el documento podremos encontrar todo lo referente a las tramas de zigbee)

1.3 Comparación de parámetros técnicos tabla comentarios

Se muestra a continuación cómo se comportan las tecnologías explicadas, se tratará de hacer lo más completa posible.

Tabla 2. Comparación de conexiones Wi-Fi y ZigBee. Tomado de:
" http://www.sase.com.ar/2012/files/2012/09/Comparativa.pdf"
(*A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fiand Wi-Fi Information & Communications Research Labs, Industrial Technology Research Institute (ITRI), Hsinchu,Taiwan*)

Estándar	ZigBee	Wi-Fi
IEEE	802.15.4	802.11
Frecuencia de banda	**868/915 MZz, 2.4GHz**	**2.4 GHz, 5GHZ**
Velocidad máxima de la señal	260Kbps	54 Mb/s
Rango nominal	10 – 100 m	100 m
Potencia TX normal	(-25) – 0 dBm	15 – 20 dBm
Número de canales de RF	1/10: 16	14(2.4GHz)
Canal de ancho de banda	0.3/0.6 MHz;2 MHz	22MHz
Tipo de modulación	BPSK(+ASK).0-QPSK	BPSK,QPSK COFDM,CCK,M-QAM
Extensión	DSSS	DSSS,CCK,OFDM
Mecanismo de convivencia	Selección de frecuencia dinámica	Selección de frecuencia dinámica control de transmisión de potencia(802.11h)
Célula básica	Estrella	BSS
Extensión de la célula básica	Grupo de árboles, malla	ESS
Número máximo de nodos de células	>6500	2007
Cifrado	AES de cifrado de bloque CTR, modo de contador	Flujo RC4 de cifrado (WEP)
Autenticación	CBC-MAC (ext de CCM)	WPA2(802.11i)
Protección de datos	16-bit CRC	32-bit CRC

La tabla cuenta con datos específicos sobre las características de cada tecnología de comunicación.

Detallaremos, rangos de frecuencias, anchos de banda, velocidad, distancia, cantidad de nodos que se podrían instalar. Se proporciona la definición de cada término para mayor claridad en la construcción de la tabla

Frecuencia de banda: Esto es intervalos de frecuencia del espectro electromagnético asignados a diferentes usos dentro de las radiocomunicaciones, su utilización es regulada por la Unión Internacional de Telecomunicaciones.

Velocidad máxima de señal: Es la velocidad en la que se transmitirá la señal que se mide en miles de baudios o mega baudios.

Rango nominal: Es el valor mínimo y máximo en distancia que cubre la señal.

Potencia TX normal: Es la energía irradiada la cual se da de la siguiente forma, Energía irradiada (dBm) = energía de transmisión (dBm)-pérdida de cable(dB)+ganancia de antena(dBi).

Canal de ancho de banda: Mejora la capacidad de redes de malla inalámbrica hay varios dispositivos que pueden transmitir en paralelo dentro de un dominio de colisión en cales distintos.

Tipo de modulación: Existen dos tipos de modulación, la analógica que se realiza a partir de señales analógicas de información por ejemplo, la voz humana, audio y video en su forma eléctrica; el segundo tipo modulación digital, que se lleva a cabo a partir de señales generadas por fuentes digitales, por ejemplo, una computadora.

Extensión: El IEEE 802.11b es un sistema de secuencia directa Spread Spectrum (DSSS) muy similar en concepto para el Wireless CDMA, utilizando una secuencia de chips de espectro ensanchado. En el 802.11b la transmisión medio es la tecnología inalámbrica y la banda de frecuencia de funcionamiento es de 2.4GHz. 802.11b proporciona 5,5 y 11 Mbps de carga útil, Velocidades de datos, además de las tarifas 1 y 2 Mbps proporcionados por 802.11. Proporcionar las tasas más altas, 8 chips Complementary Code Keying (CCK) se emplea como el esquema de modulación.

Mecanismo de convivencia: Diferentes sistemas inalámbricos que comparten la misma banda de frecuencia y de funcionamiento en el mismo entorno son propensos a interferir unos con otros y experimentar una disminución severa en el rendimiento. Consideramos 802.11 WLAN y Bluetooth basado WPAN IEEE, que operan en las bandas ISM de 2,4 GHz. Proponemos dos mecanismos de convivencia basada en técnicas de programación de tráfico, que mitigan la interferencia entre las dos tecnologías. Los algoritmos propuestos se pueden aplicar ya sea cuando 802.11 y Bluetooth son capaces de intercambiar información, así como cuando operan independientemente uno de otro. Los resultados muestran que a través de los mecanismos de coexistencia propuestas, se puede reducir la interferencia entre 802.11 y Bluetooth y el rendimiento de los dos sistemas se mejora significativamente a expensas de un pequeño retardo adicional en la transmisión de tráfico de datos.

Célula básica: Bluetooth (a través de IEEE 802.15.1), ultra-wideband (UWB, sobre IEEE 802.15.3), **ZigBee (IEEE 802.15.4 más)** y **Wi-Fi (IEEE 802.11 más)** son cuatro normas de protocolo para las comunicaciones inalámbricas de corto alcance con bajo consumo de energía. Desde el punto de vista de aplicación, bluetooth está destinado a un ratón inalámbrico, teclado y manos libres, UWB está orientado a enlaces multimedia de gran ancho de banda, **ZigBee está diseñado para redes de vigilancia y control de redes inalámbricas confiables** y, mientras que **Wi-Fi es dirigida a las conexiones de computadora a computadora** como una extensión o sustitución de las redes cableadas.

Extensión de la célula básica: Bluetooth y **IEEE 802.11 (Wi-Fi)** son dos estándares de protocolos de comunicación que definen una capa física y una capa MAC para las comunicaciones inalámbricas dentro de un rango corto (desde unos pocos metros hasta 100 m) con bajo consumo de energía (de menos de 1 mW hasta 100 mW). Bluetooth está orientado a la conexión de dispositivos de cierre, que sirve como un sustituto de los cables, mientras que **Wi-Fi está orientado a conexiones de ordenador a ordenador,** como una extensión o sustitución de cableado LAN.

Número máximo de nodos de células: Bluetooth (a través de IEEE 802.15.1), ultra-wideband (UWB, sobre IEEE 802.15.3), ZigBee (IEEE 802.15.4 más) y **Wi-Fi (IEEE 802.11 más) son cuatro normas de protocolo para las comunicaciones inalámbricas de corto alcance con bajo consumo de energía.** Desde el punto de vista de aplicación, bluetooth está destinado a un ratón inalámbrico, teclado y manos libres, UWB está orientado a enlaces multimedia de gran ancho de banda, **ZigBee está diseñado para redes de vigilancia y control de redes inalámbricas confiables** y, mientras que **Wi-Fi**

es dirigida a las conexiones de computadora a computadora como una extensión o sustitución de las redes cableadas.

Cifrado: Se presenta un nuevo tipo de interferencia electromagnética intencional (IEMI) que provoca la fuga de información de la ICS criptográficos (circuitos integrados). Como una amenaza reciente, se sabe que los fallos en circuitos integrados criptográficas tales como Advanced Encryption Standard (AES) tienen una influencia significativa sobre las fugas de información sensible. AES es un cifrado de bloques estandarizados por el NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos), que es un estándar de-facto de los circuitos integrados de tarjetas inteligentes y se utiliza para muchos dispositivos de seguridad

Autenticación: Negocios basados en la red, incluidos los servicios financieros en línea han sufrido varios ataques a la autenticación de usuarios. Hay un fuerte deseo de desarrollar y poner en práctica esquemas de autenticación más seguros para proteger a las empresas y clientes contra las amenazas de seguridad. El trabajo intensivo que se ha hecho en esta área, para mejorar la autenticación de contraseña tradicional, como esquema de intercambio de clave de autenticación de dos factores, la sesión, y el esquema de contraseña dinámica. Sin embargo, estos planes no se han demostrado su eficacia, debido a su diseño de seguridad o gastos adicionales. A diferencia de la autenticación de la contraseña tradicional (donde se utiliza una contraseña estática) o autenticación de dos factores (donde se requieren dos piezas de información de autenticación), utilizar una contraseña de una sola vez dinámica (OTP), basado en la contraseña del usuario, el tiempo de autenticación, así como una propiedad única que posee el usuario en el momento de la autenticación (es decir, "algo que el usuario tiene", por ejemplo, la dirección MAC de la máquina que el usuario utiliza para la autenticación).

Protección de datos: La protección y la verificación, que la integridad permanece intacta, de los datos almacenados e intercambiados en los sistemas electrónicos, se ha investigado durante décadas. Que los datos han evolucionado para incluir el código embebido de máquinas, previamente restringido a la carga en los depósitos o en ambientes controlados. Además, hay una discusión sobre el uso de una técnica de legado para verificar una,-código de la máquina de campo cargado.

Los protocolos 802.11b/g, son adecuados para operar con RFID, ya que, éste sólo necesita el ancho de banda para trazabilidad es un monitoreo de los equipos en tránsito, que significa en ciertos periodos de tiempo se estaría censando los equipos para controlar

la ubicación a la vez no requiere mucho recurso en ancho de banda.(sólo aplica para activas y semi-activas)

La información de la tabla 2 fue tomada de un ciclo de conferencia dada en la ciudad de Taipe - Taiwan, en el año 2007, para mayores datos se puede consultar.

Published in:
Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE

Date of Conference: 5-8 Nov. 2007
Page(s): 46 - 51
ISSN: 1553-572X
Print ISBN: 1-4244-0783-4
INSPEC Accession Number: 9848735

Conference Location: Taipei
Digital Object Identifier: 10.1109/IECON.2007.4460126

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4460126&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4460126.

Segunda etapa
Propuesta del sistema automático de trazabilidad para la UDB-CS

2.1 Contextualizando UDB-CS general – específica relación con los sistemas de conectividad

Actualmente la UDB-CS cuenta con un sistema de conexión de red inalámbrica con tecnología WiFi. A continuación se detalla con una tabla las redes existentes:

Tabla 3. Especificación de redes UDB-CS

ZONA	REDES	DESCRIPCIÓN
Edificio R	Estudiantes PublicaR EstudiantesA Edificio A Network Publicidad	Se ha considerado, solamente las instalaciones de la Universidad Don Bosco, separadas las redes por edificio, más adelante se realizara una medición de potencia en base a decibeles. Identificamos las Redes abiertas (Pública, Estudiantes, EstudiantesA, EstudiantesB, PublicaR, EdificioC. Las demás redes son seguras con clave de ingreso, la cual es asignada por Soporte Técnico
Edificio A	APDAF PublicaR Edificio A Network EstudiantesA	
Edificio B	EstudiantesB TMA PublicaR	
Edificio C	EdificioC WCDIU1 WCDIU2 WCDIU3	
EX-SUM	Docentes Estudiantes Pública Catedráticos HP835300	
CDIU	WCDIU1 WCDIU3 DLINK EDIFICIOC	

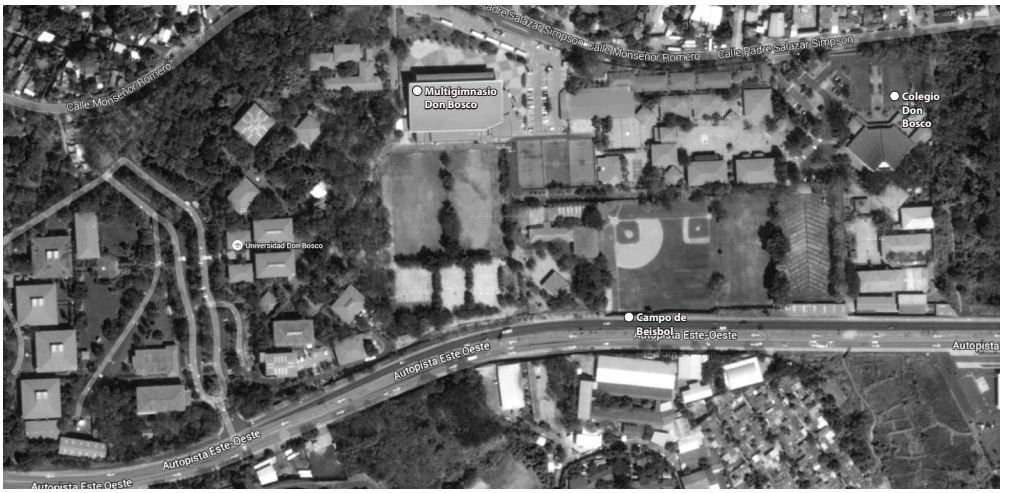


Imagen 1. Satelital de la Ciudadela Don Bosco, identificando la Universidad, El Colegio y las instalaciones del CITT

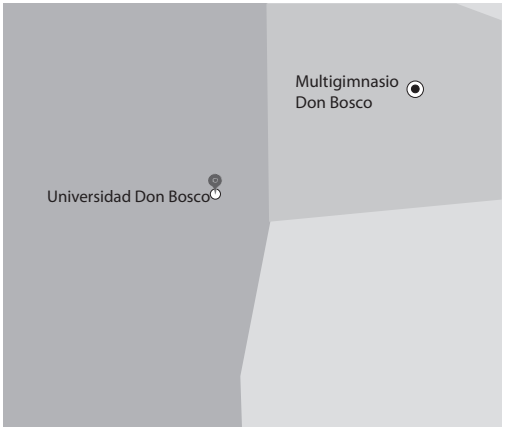


Imagen 2. Campus de la Universidad Don Bosco, que es el área de estudio

Se incluye al Multigimnasio, este es administrado por la Universidad Don Bosco. El área total del campus es de 15 manzanas asignadas para saber la cantidad de metros cuadrados debemos hacer la conversión correspondiente.

1 manzana es a 6987.3878 metros ^{2,}
15 manzanas es a X
X = (15 manzanas * 6987.3878 metros ^{2})/ 1manzana. Eliminamos manzanas y nos quedan metros cuadrados.
X = 104,810.817 metros ^{2}

Debemos cubrir los diferentes accesos al campus que están ubicados en caceta norte ingreso de vehículos más peatonal, caceta sur ingreso de vehículos más peatonal, caceta Multigimnasio ingreso de vehículos más peatonal, existe otro acceso pero este es por la casa de los padres vehículos sólo autorizados y peatonal, los visitantes en dichos ingresos deben dejar una identificación para que se les entregue un carné de visitante, el cual debe ser colocado en un lugar visible. En la siguiente imagen de satélite se identificarán los accesos mencionados.

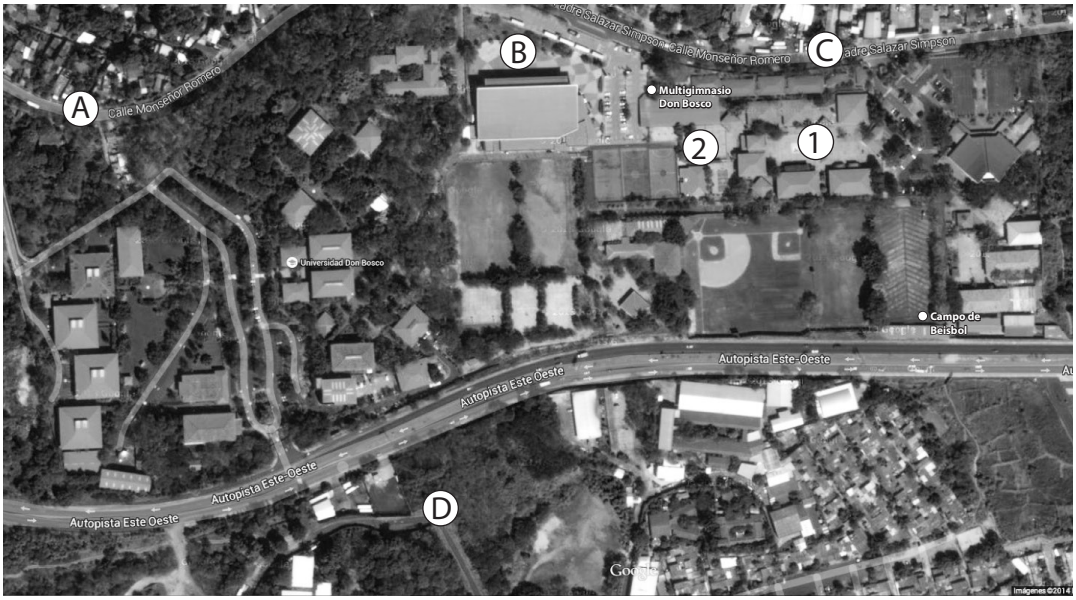


Imagen 3. Satelital con puntos claves UDB-CS.

Detalle	
A: Caceta Sur	1: Acceso al Colegio Don Bosco
B: Entrada Peatonal	2: Canchas de futbol rápido
C: Entrada Mutigimnasio	
D: Caseta Norte	

El ingreso por el Multigimnasio, tiene una entrada más que da acceso al Colegio Don Bosco, los estudiantes de la Universidad caminan ese tramo y luego pasan las canchas de futbol y básquetbol, para ingresar por el área de Cafetería a las instalaciones de la Universidad.

Las señales abiertas están reservadas para el uso de visitas y alumnos, he inclusive el personal de la universidad puede acceder a ellas, pero la comunicación y la navegación es débil, a medida que los equipos se alejan del AP, se requiere de más potencia y la señal se desvanece; por lo que la comunicación se pierde.

Esta imagen que muestra la ubicación de los diferentes edificios de la Universidad más Estudios tecnológicos, llegando hasta el Multigimnacio, nos ha servido para hacer un mapeado de las señales de las diferentes redes WiFi. En consecuencia podemos mencionar lo siguiente:

En el siguiente tema, se muestra los cálculos realizados para determinar los decibeles con los que cuentan las diferentes redes de la UDB-CS.

2.2 Metodología de medición y aspectos a medir.

Mediciones Intensidad de Potencia de Señal WIFI – UDB
Baja: 0 –19 (Porcentaje de Intensidad de Señal)
Regular:20 – 39
Media: 40 – 59
Intermedia: 60 – 79
Excelente: 0 – 100

Formula: $P_w = \frac{1}{1000} .10^{\frac{x}{10}}$; *x Valor de Potencia en dBm*

Potencia

Todas las mediciones se realizaron tomando en cuenta la intensidad de la señal, potencia, distancia del AP, en ambos casos, para ello se tomó más de una muestra para la medición.

Existe un margen de error el cual, está determinado por el tipo de tarjeta inalámbrica que posea el equipo que desee conectarse a una de las redes inalámbricas presentadas en las siguientes tablas.

Tabla 4. Medición de potencia en dB por red WiFi instalada en la UDB-CS

Medición – Edición EXSUM				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Catedráticos	62%	Intermedia	-56 dBm	2.51 pW
Docentes	100%	Excelente	-30 dBm	1.0 mW
Estudiantes	40%	Media	-71 dBm	0.079 pW
Public	66%	Intermedia	-53 dBm	5.01 pW

Medición – Edición EXSUM (Alrededores) – Parte I				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Catedráticos	82%	Excelente	-56 dBm	2.51 pW
Docentes	100%	Excelente	-30 dBm	1.0 mW
Estudiantes	44%	Media	-69 dBm	0.1258 pW
Public	92%	Excelente	-36 dBm	0.2511 mW

Medición – Edición EXSUM (Alrededores) – Parte II				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Catedráticos	82%	Excelente	-56 dBm	2.51 pW
Docentes	100%	Excelente	-30 dBm	1.0 mW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Public	92%	Excelente	-36 dBm	0.2511 mW

Medición – Cafetería Arriba				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Public	52%	Media	-63 dBm	0.5011 pW
Estudiantes	28%	Regular	-80 dBm	0.01 pW
WCDIU	20%	Baja	-85 dBm	0.0031 pW
EDIFC	18%	Baja	-86 dBm	0.0025 pW

Medición – Cafetería Arriba – Parte II				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW
WCDIU	40%	Media	-71 dBm	0.0794 pW
EDIFC	14%	Baja	-89 dBm	0.0012 pW

Medición – Cafetería Abajo				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW
WCDIU	40%	Media	-71 dBm	0.0794 pW
EDIFC	20%	Baja	-85 dBm	0.0031 pW

Medición – Cafetería Abajo – Parte II				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW
WCDIU	50%	Media	-64 dBm	0.3981 pW
EDIFC	24%	Regular	-82 dBm	0.0063 pW

Medición – Parqueo CDIU				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW
WCDIU	50%	Media	-64 dBm	0.3981 pW
EDIFC	24%	Regular	-82 dBm	0.0063 pW

Medición – CDIU & Edificio C				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EDIFC	100%	Excelente	-30 dBm	1.0 mW
WCDIU	86%	Excelente	-40 dBm	100 pW
Docentes	70%	Intermedia	-51 dBm	7.94 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW

Medición – CDIU Primera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	100%	Excelente	-30 dBm	1.0 mW
EDIFC	100%	Excelente	-30 dBm	1.0 mW
Docentes	70%	Intermedia	-51 dBm	7.9432 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Catedráticos	54%	Media	-62 dbm	0.6309 pW
Public	52%	Media	-63 dBm	0.5011 pW

Medición – CDIU Segunda Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	100%	Excelente	-30 dBm	1.0 mW
EDIFC	100%	Excelente	-30 dBm	1.0 mW
Docentes	70%	Intermedia	-51 dBm	7.9432 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW

Medición – CDIU Tercera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	100%	Excelente	-30 dBm	1.0 mW
EDIFC	100%	Excelente	-30 dBm	1.0 mW
Docentes	70%	Intermedia	-51 dBm	7.9432 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW
Public	52%	Media	-63 dBm	0.5011 pW

Medición – Edificio C				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	100%	Excelente	-30 dBm	1.0 mW
EDIFC	100%	Excelente	-30 dBm	1.0 mW
Docentes	70%	Intermedia	-51 dBm	7.9432 pW
Estudiantes	66%	Intermedia	-53 dBm	5.01 pW

Medición – Edificio C Primera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	100%	Excelente	-30 dBm	1.0 mW
EDIFC	100%	Excelente	-30 dBm	1.0 mW
Estudiantes	76%	Intermedia	-47 dBm	0.0199 mW
Docentes	70%	Intermedia	-51 dBm	7.9432 pW

Medición – Edificio C Segunda Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Estudiantes	100%	Excelente	-30 dBm	1.0 mW
EDIFC	54%	Intermedia	-62 dBm	0.6309 pW
Docentes	38%	Regular	-73 dBm	0.0501 pW
WCDIU	30%	Regular	-78 dBm	0.158 pW

Medición – Edificio B & Edificio C				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
WCDIU	58%	Media	-59 dBm	0.0012 mW
EstudiantesB	36%	Regular	-74 dBm	0.0398 pW
EDIFC	22%	Regular	-84 dBm	0.0039 pW
Estudiantes	20%	Regular	-85 dBm	0.0031 pW
Docentes	14%	Baja	-89 dBm	0.012 pW

Medición – Edificio B Primera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EstudiantesB	32%	Regular	-77 dBm	0.0199 pW
EstudiantesA	28%	Regular	-80 dBm	0.01 pW

Medición – Edificio B Segunda Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EstudiantesB	46%	Media	-67 dBm	0.1995 pW
EstudiantesA	42%	Media	-70 dBm	0.1 pW
Docentes	28%	Regular	-80 dBm	0.01 pW
Estudiantes	26%	Regular	-81 dBm	0.0079 pW

Medición - Edificio B Tercera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EstudiantesA	44%	Regular	-69 dBm	0.1258 pW
EstudiantesB	34%	Regular	-75 dBm	0.0316 pW

Medición - Plaza				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EstudiantesA	88%	Excelente	-38 dBm	0.1584 pW
Edificio A Network	54%	Media	-62 dBm	0.6309 pW
Docentes	50%	Media	-64 dBm	0.3981 pW
EstudiantesB	44%	Media	-69 dBm	0.1258 pW
Public	38%	Regular	-73 dBm	0.0501 pW
Catedraticos	24%	Regular	-82 dBm	0.0063 pW
EDIFC	16%	Baja	-88 dBm	0.0015 pW

Medición - Edificio A Primera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Edificio A Network	56%	Media	-60 dBm	0.001 mW
EstudiantesA	40%	Media	-71 dBm	0.0794 pW

Medición - Edificio A Segunda Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Edificio A Network	100%	Excelente	-30 dBm	1.0 mW
EstudiantesA	68%	Intermedia	-52 dBm	0.0063 mW
EstudiantesB	24%	Regular	-82 dBm	0.0063 pW
Docentes	22%	Regular	-84 dBm	0.0039 pW
PublicR	22%	Regular	-84 dBm	0.0039 pW
Public	20%	Regular	-85 dBm	0.0031 pW

Medición - Edificio A Tercera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Edificio A Network	62%	Intermedia	-56 dBm	0.0025 mW
EstudiantesA	44%	Media	-69 dBm	0.1258 pW
PublicR	30%	Regular	-78 dBm	0.0158 pW
Docentes	22%	Regular	-84 dBm	0.0039 pW

Medición - Edificio R Primera Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
APDAF	86%	Excelente	-40 dBm	0.1 mW
PublicR	62%	Intermedia	-56 dBm	2.5118 pW
Edificio A Network	38%	Regular	-73 dBm	0.0501 pW
Estudiantes	28%	Regular	-80 dBm	0.01 pW
Publicidad	26%	Regular	-81 dBm	0.0079 pW

Medición - Edificio R Segunda Planta				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Edificio A Network	52%	Media	-63 dBm	0.5011 pW
Estudiantes	48%	Media	-66 dBm	0.2511 pW
PublicR	44%	Media	-69 dBm	0.1258 pW
EstudiantesA	32%	Regular	-77 dBm	0.0199 pW
BiblioAP	26%	Regular	-81 dBm	0.0079 pW
APDAF	24%	Regular	-82 dBm	0.0063 pW

Medición - Biblioteca				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
BiblioAP	84%	Excelente	-41 dBm	0.0794 mW
Estudiantes	74%	Intermedia	-48 dBm	0.0158 mW
PublicR	22%	Regular	-84 dBm	0.0039 pW

Medición - Capilla				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
PublicR	44%	Media	-69 dBm	0.1258 pW
Publicidad	42%	Media	-70 dBm	0.1 pW
EstudiantesA	40%	Media	-71 dBm	0.0794 pW
BiblioAP	32%	Regular	-77 dBm	0.0199 pW
Edificio A Network	16%	Baja	-88 dBm	0.0015 pW

Medición - Glorietas Capilla				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
EstudiantesB	42%	Media	-70 dBm	0.1 pW
EstudiantesA	40%	Media	-71 dBm	0.0794 pW
Docentes	38%	Regular	-73 dBm	0.0501 pW
Public	32%	Regular	-77 dBm	0.01995 pW
Catedraticos	30%	Regular	-78 dBm	0.0158 pW
EDIFC	20%	Regular	-85 dBm	0.0031 pW
PublicR	18%	Baja	-86 dBm	0.0025 pW

Medición - Glorietas EXSUM				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	96%	Excelente	-33 dBm	0.5011 mW
Public	70%	Intermedia	-51 dBm	0.0079 mW
Catedráticos	62%	Intermedia	-56 dBm	0.0025 mW
EstudiantesA	44%	Media	-69 dBm	0.1258 pW
EstudiantesB	24%	Regular	-82 dBm	0.0063 pW

Medición - Bodega				
	Intensidad de la Señal	Intensidad de la Potencia	Potencia de la Señal (dBm)	Potencia de la Señal (W)
Docentes	54%	Intermedia	-62 dBm	0.6309 pW
Public	42%	Media	-70 dBm	0.1 pW
Catedraticos	34%	Regular	-75 dBm	0.0316 pW
EstudiantesA	24%	Regular	-82 dBm	0.0063 pW
EstudiantesB	22%	Regular	-84 dBm	0.0039 pW
Estudiantes	20%	Regular	-85 dBm	0.0031 pW

Identificando la nomenclatura se tiene:

En telecomunicaciones es muy común tener que hablar de potencia de una señal (potencia transmitida o potencia recibida) y de atenuación de una señal (conocer cuánto se atenúa una señal a lo largo de un enlace), las unidades que se utilizan son.

pW: pico watts (La cantidad de potencia producida por una célula o módulo bajo las condiciones nominales de irradiación (STC)) 1 X 10^{-12} W
mW: mili watts (1 X 10^{-3})Watts

Para el caso, la lectura de pW sería 0.000000000001 watts y para mW sería de 0.001 watts, para estandarizar los cálculos se usa la escala logarítmica. Así, cambia la escala a decibeles y se define como diez veces el logaritmo en base diez de una cierta magnitud:

$$10 \times \log(x) \text{ decibel}$$

Por lo que se usa el símbolo dB para identificar al decibel, a partir de dicha definición se especifica la siguiente unidad:

$$[dBW] = 10 \times \log (x/1 \text{ watt})$$

El dB-watt de la nueva ecuación en 10 veces el logaritmo de una potencia expresada en watts (referida a 1 watt de potencia). Esto significa que una señal que tiene una potencia de 1 watt es equivalente a una potencia de 0 dBW.

Como sería el dB –miliwatt en este caso:

$$[dBm] = 10 \times \log (x/1 \text{ miliwatt})$$

Que podemos decir entonces, 0 dBm equivale a 1 miliwatt. Ejemplo 1000 miliwatts equivaen a 30 dBm. O lo que es igual a 1 watt también equivale a 30 dBm.
En Cambio, 0.001 watt equivalen a -30 dBw. Dicho de otro modo, 1 miliwatt también equivale a -30 dBW.

La atenuación de la señal está definida por:

$$\text{Atenuación [dB]} = 10 \times \log (\text{Potencia de entrada/Potencia de salida})$$

2.3 Tabla de resultados comentada

Se utilizó un software para las mediciones de señal en cada área de la universidad, **VISTUMBLER,** entre más cerca nos encontramos de los AP, mejor es la señal, pero entre más nos alejamos de ellos se necesita mayor potencia para tener una recepción aceptable. Dichas mediciones indican que la red WiFi no es confiable en puntos alejados de los AP, esto es porque se necesita mayor potencia para tener una buena recepción,

considerando que la señal se atenuaría por obstáculos tales como, paredes y árboles que circundan la universidad.

En consideración a lo anterior, se colocarían equipos RFID en cada planta de los edificios con a una distancia de 10 metros. Con ellos podemos mantener un control efectivo de los equipos móviles con los que cuenta la universidad. La cantidad de equipos instalados por planta sería de 3 distribuidos de la siguiente manera.

a. A la altura de las gradas
b. Al centro de los pasillos

Con esto se podrá monitorear los equipos y poder tener trazabilidad.

Se tendrá un control efectivo del personal que manipula los equipos, cuando estos se movilicen fuera de las aulas y pasillos, se colocarían AP Zigbee para cubrir la necesidad de trazabilidad entre edificios, se propone que la señal Zigbee, cubra las diferentes casetas de ingreso a la universidad, pero la forma operativa del personal de vigilancia debe cambiar, ya que ante una señal, en la que se determine que un componente esté móvil este por salir de las instalaciones, el personal debe interceptar y revisar si dichos equipos cuentan con la documentación correspondiente que avale su salida del UDB-CS.

Luego de ello, el personal correspondiente deberá informar a las autoridades correspondientes para las sanciones necesarias. Este sistema de monitoreo es tan efectivo que se puede colocar tag activos a cada vehículo, motocicletas y bicicletas, dando un plus más a los bienes de la universidad.

En el capítulo tres, analizaremos la tecnologías RFID, con la finalidad de poder tener más elementos de decisión, no debemos olvidar que una institución educativa, no siempre cuenta con los recursos económicos suficientes para una adquisición para ejecutar un proyecto de esta envergadura, pero hay que considerar que la UDB-CS, ya cuenta con parte de una tecnología instalada, esta es la WiFi, que abarca casi todo el campus.

Esta infraestructura instalada WiFi, se utilizará para la solución al problema planteado. Procederemos a indicar la solución propuesta en el capítulo tres apartado 3.3. La cual, radicará en la ubicación de las antenas, interconexión entre los equipos RFID y WiFi en cada edificio, mientras que RFID con Zigbee se realizará en los espacios que cubran más terreno.

El sistema de monitoreo por radio frecuencia RFID, se puede utilizar en todo tipo de problemática, tal como: Control de acceso a recintos, seguimiento de materia prima si lo vemos para la industria o producto terminado, control de personal, control de vehículos institucionales.

.

Tercera etapa
Arquitectura física de un sistema automatizado de trazabilidad con RFID

Analizaremos en cada una de las etapas las características de las tecnologías de comunicación propuestas, es este momento iniciaremos con la estructura RFID que se ofrece como una solución para el control de los bienes móviles de la UDB-CS. Que se podrían instalar, como parte de la solución.

3.1 RFID

¿Qué es RFID?
Un sistema RFID (Radio Frequency IDentification), es una tecnología inalámbrica que nos permite, básicamente, la comunicación entre un lector y una etiqueta.

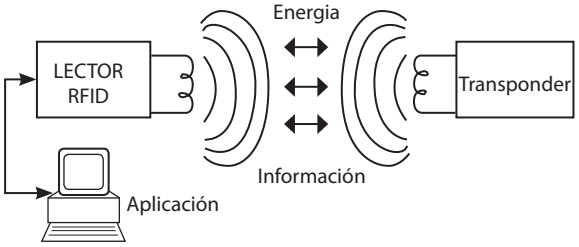


Figura 5. Esquema de un sistema RFID

Observemos un diagrama simple de cómo funciona el RFID, contaríamos con una aplicación informática, la cual se encargaría de llevar el registro de los equipos o bienes que se estén monitoreando, luego esta aplicación se conectaría a los lectores quienes mandan una señal de radio frecuencia la cual es recibida por los transponder.

Considerando lo anterior, vemos que el transponder "tag", que también se conoce como etiqueta electrónica contiene un microchip y una antena, que puede adherirse a cualquier producto.

El microchip almacena un número de identificación único para los bienes que se desean controlar; pero como hace esto de poder controlar varios equipos en un solo tag; cada equipo RFID cuenta con un sistema anticolisión que permiten leer varias tarjetas el mismo tiempo. Esto sucede cuando varias tarjetas se encuentran en el rango de acción del interrogador y dos o más quieran transmitir al mismo tiempo. En ese momento se produce una colisión, esta es detectada por el interrogador y manda parar la transmisión de las tarjetas durante un tiempo[8].

El funcionamiento de los dispositivos de RFID, se realiza entre los 50KHz y 2.5 GHz. Las unidades que funcionan a bajas frecuencias (50KHz a 14MHz) son de bajo costo, corto alcance y resistencia al ruido. Mientras que los que trabajan a altas frecuencias en los rangos (14MHz a 2.5GHz), son sistemas de mayor valor monetario y tecnología más compleja.

La etiqueta contiene información que puede ser sólo o puede permitir la escritura, dependiendo del tipo de memoria que posee el transporder. La mayor parte de los sistemas tienen memoria EEPROM[9], en ocasiones hay datos pregrabados de fábrica y en otros se puede grabar por parte del usuario. Los usuarios reciben esta información en un lector portátil con un display alfanumérico o puede pasar directamente a un ordenador que procese los datos obtenidos.

Un sistema RFID, tiene multitud de aplicaciones, se puede usar como tarjetas identificadoras sin contacto, un uso de este tipo se puede ver por ejemplo, en el sistema de pago utilizado en peajes llamado viaT[10].

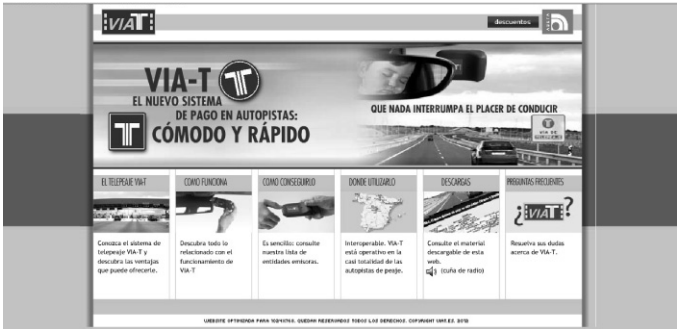


Figura 6. Pago en autopista

8. Ciudad, Herrera. J.M., Casanovas, E. S, Estudio, diseño y simulación de un sistema de RFID basados en EPC, Página 9, https://docs.google.com/file/d/0B1aK7vZILIBdNEZCR3NWUmF3aU0/edit
9. EEPROM, Electrically Eraseble Programmable Read-Only Memory
10. viaT: http://www.viat.es/

- Dicho sistema ofrece la oportunidad de que el vehículo no se detenga en los accesos a edificios oficiales o a empresas privadas.
- Otra aplicabilidad es la inmovilización de vehículos, que consisten en un sistema interrogador situado en el vehículo a proteger y en un identificador en la llave.
- Quizá uno de los usos más frecuentes es la identificación de paquetes en un almacén o bodega.

Y así podemos ir detallando más aplicabilidades de dicho sistema.
En consecuencia, estas aplicaciones aportan muchas ventajas. Entre ellas están:

- Conocer el historial médico de personas con dolencias especiales o delicadas que deberían tener un control especial al momento de un percance.
- Tener un control del personal de una institución o empresa, conociendo su ubicación real.
- Controlar los bienes de las empresas, que con mucho esfuerzo ha sido adquirido.
- E incluso se puede monitorear a las visitas que llegan, observando por medio de su trazabilidad si realmente se dirigen a donde ellas han mencionado ir, para instalarse de forma independiente en entornos industriales interiores, los módulos de solución:

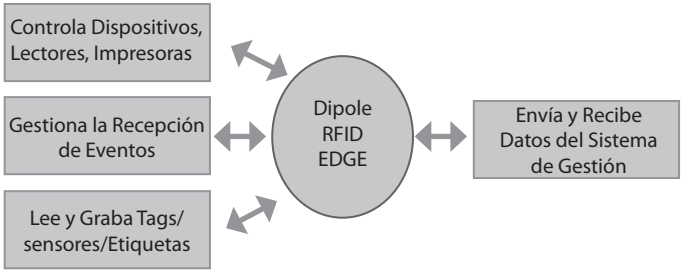


Figura. 7. Esquemática del funcionamiento de un sistema RFID

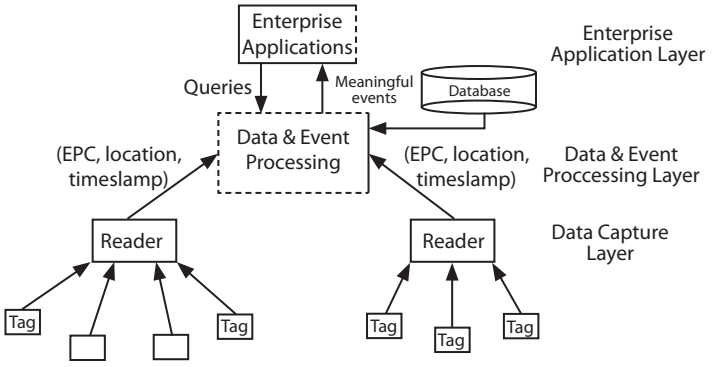
La señal recibida por el interrogador desde la tarjeta está a un nivel de -60 db por debajo de la portadora de transmisión. El rango de lectura para la mayoría de los casos está entre los 30 y 60 centímetros de distancia entre interrogador y tarjeta.

Podemos encontrar además dos tipos de interrogadores diferentes:

1. Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.
2. Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más caros, pero consiguen unas prestaciones mayores.

3.2 Arquitectura RFID

Figura 8. Arquitectura de un sistema RFID, tomado del artículo: RFID Data Management, Aggregation and Filtering, Olekasandr Mylyy



Todo sistema RFID se compone de un interrogador o sistema de base que lee y escribe datos en los dispositivos y un transponder o transmisor que responde al interrogador.

1-El interrogador genera un campo de radiofrecuencia, normalmente conmutando, una bobina a alta frecuencia. Las frecuencias usuales van desde 125 Khz hasta la banda ISM de 2.4 Ghz, incluso más.

2-El campo de radiofrecuencia genera una corriente eléctrica sobre la bobina de recepción del dispositivo. Esta señal es rectificada y de esta manera se alimenta el circuito.

3-Cuando la alimentación llega a ser suficiente el circuito transmite sus datos.

El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal.

Trazabilidad.

La trama de RFID, está dada para tener una comunicación entre los equipos en movimientos más el personal encargado de su manejo. Se generará una verificación de control acorde a la detección realizada, puede ser por una o más antenas receptoras.

Elementos de trama de detección de movimiento

Identificador Tipo Señal -> Ids (4 para señales de detección de movimiento)
Identificador UDB-CS -> Idc
Identificador de Antena (Área) -> Ida
Numero personas -> Np

Construcción de la trama
Ids-Idc-Ida-Np

Ejemplo: 4-34-3-5

IDS	IDC	IDA	NP
4	34	3	5

3.3 Propuesta de solución acorde a los parámetros

Recordar lo expuesto, sobre las características que se buscan en un sistema RFID.

Tags (transponders o etiquetas electrónicas): Son los elementos identificadores del objeto. Evidentemente, su tamaño deberá estar en relación con el objeto a identificar (pueden ser inferiores al centímetro). No es necesario que sean "visibles" al lector. Se distingue entre activos, que incorporan una batería que les permite transmitir de forma autónoma, y pasivos, en los que la energía que necesitan la reciben del lector en la onda trasmitida. Otra subdivisión es entre tags de solo lectura, con un número único grabado de fábrica, y de lectura-escritura, en los cuales se puede grabar información para ser leída posteriormente también por radio frecuencia. Se componen de una electrónica y una antena. La distancia a que pueden ser leídos varía entre un máximo de 90/100 centímetros para los pasivos hasta los 100 metros de algunas soluciones activas.

Lector: Es el equipo electrónico que se comunica con el tag y captura la información que contenga. Habrá de ser compatible con el tag y sobre todo, trasmitir en la misma frecuencia de banda. Los lectores se integran en el sistema a través de una CPU, normalmente cualquier ordenador, por diferentes conexiones estándar (serie 232 o 485, ethernet). Estos lectores suelen ser fijos (para instalar en un punto concreto), si bien hay diversas soluciones susceptibles de integrarse en dispositivos móviles (lectores en formato PCMCIA o Compact Flash).

Antena: Trasmite y recibe la señal generada por el lector. CPU: En alguna ocasión está integrada en el lector, si bien, lo habitual, es disponer de un ordenador personal (o un terminal con ranura PCMCIA para los lectores móviles) que integre la información en la red de la empresa.

Software: Dependiendo de cada aplicación en concreto, se suele desarrollar un software específico que optimice las posibilidades del sistema y las ventajas de la identificación automática.

Los sistemas pueden ser propietarios, todo el sistema debe ser de un mismo fabricante (normalmente los sistemas activos de alto valor añadido), o abiertos, lectores compatibles con tags de distintos fabricantes.

El costo puede variar de acuerdo al mercado internacional, los precios mostrados son de empresas extranjeras, esto lo podemos ver en el anexo 6. Tipos de equipos y sus costos.

En todo caso, la factibilidad económica se reduce en los costos de la interconexión con los equipos correspondientes de RFID y WiFi.

A que nos referimos; existe un sistema de comunicación pre-instalado, el cual da cobertura a las instalaciones de la universidad. Esto nos lleva a una reducción en costos, por lo que la universidad debe invertir es en la adquisición de los equipos RFID, en consecuencia, la inversión realmente es mínima, el costo de la elaboración de tarjetas "tag", es recuperable. Dichos tag, serían permanentes para los equipos, habría otra posibilidad no evaluada y es la de entregar a estudiantes carnés, los cuales pueden monitorearse y conocer la ubicación de los estudiantes, igual sería al momento de abrir un área, este se podría hacer con dicho carné, el pasar asistencia a una clase, las posibilidades son muchas. No se invertiría en equipos WiFi, ya que estos están instalados, sino que se invertiría en equipos RFID y ZigBee, es acá donde radicaría el mayor costo, puesto que la

inversión es alta, pero como se menciona en líneas anteriores hay diferentes formas de ir recuperando la inversión.

Las redes ZigBee y el RFID. La primera de ellas se implementaría para la infraestructura de la red de captura de datos, y la segunda, como elemento de lectura de información. A continuación, se describe el desarrollo del sistema de captura de datos.

Para este trabajo se ha desarrollado una red ZigBee en configuración en entre ella, es decir, con un coordinador de red Access Point (AP) y un total de cinco de dispositivos finales (Router/End Device) uno por máquina. En estos dispositivos finales es donde se implementarán los lectores RFID. Por lo tanto, serán los puntos donde se recogerá la información de las etiquetas. El AP se conectará directamente al puerto USB del PC y se encargará de recopilar la información de toda la red. A continuación, se describe la estructura de los elementos de la red y cuál es su configuración.

·Access Point. Para el envío de información a los Router/End Device se ha seleccionado una comunicación de tipo Broadcast, de tal manera que los paquetes de datos enviados por el AP serán recibidos por todos los elementos de la red. En las peticiones de información enviada a los Router se enviará el número de nodo (nº de máquina) al que se le realiza la petición, de tal manera que solo responderá al que pertenezca el identificador enviado.

·Estructura de los Router/EndDevice. Este tipo de nodos son los elementos de captura de datos. En este apartado se describirá cuál es el hardware y software desarrollado para implementar los dispositivos finales de la red, basados en lectores RFID. Para la implementación de los End Device son necesarios tres elementos:

1. El lector RFID. Lo primero que se hizo fue seleccionar un lector adecuado que tuviera posibilidad de comunicación, además de un precio accesible. Después de analizar distintos lectores de varios fabricantes, se optó por los lectores embebidos del fabricante Skyetek. Estos, además de tener varias salidas de comunicación (UART, SPI, USB) tienen un robusto protocolo anticolisión, que permite leer varias etiquetas simultáneamente, aspecto este último necesario para esta aplicación. El lector empleado dispone de una antena integrada.

2. El modem ZigBee. Se seleccionó el mismo modelo que para el AP, del fabricante Digi. Éstos, se programaron en modo AT, y con dirección de destino la del AP.

3. Un microcontrolador. Para comunicar el lector RFID con el modem ZigBee es necesario implementar un circuito interface entre ambos. Para la realización de las primeras pruebas se seleccionó la plataforma de hardware libre Arduino, basados en los microcontroladores de Atmel AVR. Este entorno permite desarrollar aplicaciones, bajo lenguaje C++, de forma rápida y a bajo costo.

Con lo antes expuesto, podemos afirmar que es viable realizar una conexión ZigBee con RFID y tener una trazabilidad para los bienes móviles UDB-CS, en los lugares donde no hay cobertura WiFi.

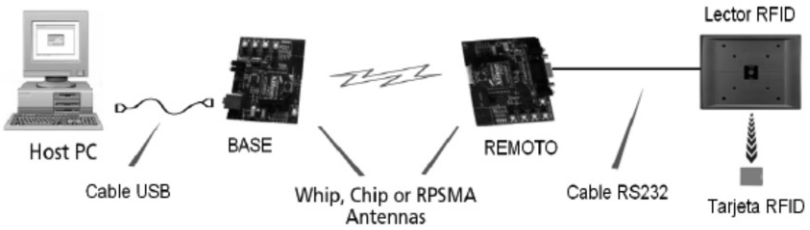


Figura 9. Conexión Zigbee con RFID

EQUIPOS ZIGBEE

Dado el problema de que la potencia de las redes instaladas en el campus son débiles y con poco alcance radial en metros es que se toma la opción:

1-Usar tres antenas ZigBee Pro para la comunicación, esta tiene un alcance de 1600 metros radiales.
2-Colocando tres antenas en puntos estratégicos se podrá controlar el campus universitario más el CITT.
3-Cuenta con las características siguientes. Protocolo 802.15.4, Banda de 2.4 GHz, Robusto en ambientes con contaminación radial, montaje fácil, cobertura de señal de 1600 metros, 300 nodos.

Antenas ZigBee propuestas para cubrir la distancia de 1600 metros en áreas sin cobertura:

- Modelo: DRF2619A
  - Color: Negro
  - Material: Aleación de aluminio de vivienda

- Voltaje: DC 5 ~ 12V
- Corrientes:> 300mA
- Puerto serie Velocidad de transmisión: 9600, 19200, 38400, 57600, 115200 bps (seleccionable)
- Por defecto: 38400 bps
- Frecuencia inalámbrica de 2.4GHz (2460MHz)
- Alcance de transmisión: 1600 metros
- Recepción de sensibilidad:-110dBm
- Chipset principal: CC2530F256, 256KFLASH
- Punto configurable: puede configurar como coordinador o router
- Viene con antena.

Los componentes RFID son utilizables para la trazabilidad de los equipos móviles.

La siguiente configuración muestra la arquitectura de conexión de la red en la UDB-CS, podemos observar que las líneas rojas indican la red de fibra óptica y la línea verde es la comunicación inalámbrica.

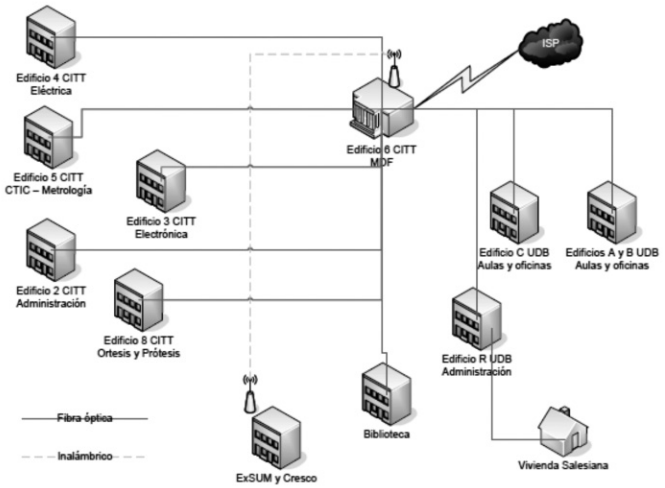


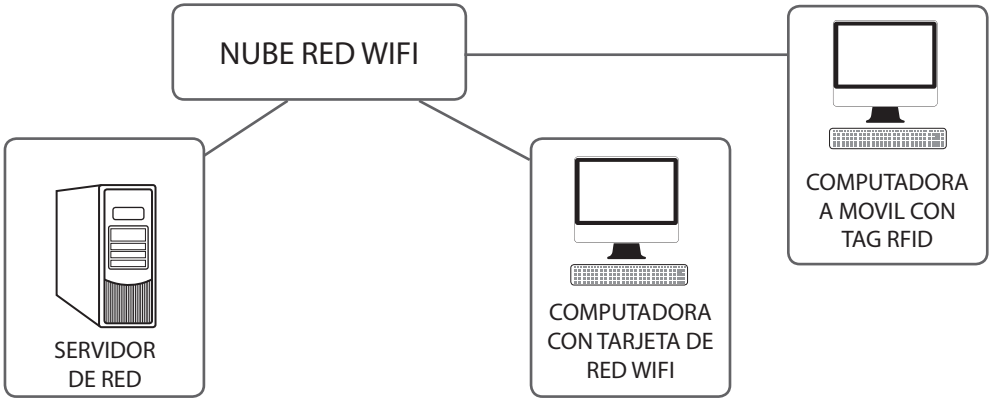
Figura 10. Distribución Física de Conexines RED UDB

Dado que la investigación reflejó áreas de la universidad donde no existe señal de la WiFi, para poder monitorear equipo en riesgo, se ofrece la siguiente configuración.

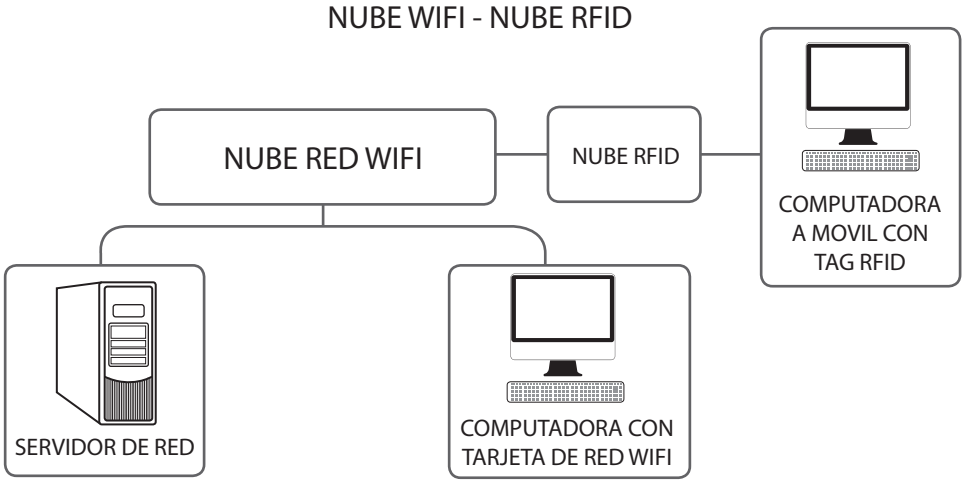
a)En las áreas donde la señal WiFi es adecuado colocar los componentes RFID para detectar los TAG de los equipos móviles.

b) En las zonas donde la señal WiFi es casi nula o total mente nula, se daría la solución de configurar equipos netamente ZIGBEE 802.15, esto ayudaría a mantener un control más efectivo y constante.

A continuación se muestra un diagrama de conexión usando WiFi - RFID.



La Figura 11.
Representa una conexión WiFi con RFID simple, de tal forma que no se advierte la conexión RFID.



En la Figura 12. Podemos observar la nube RFID interactuando con la nube WiFi.

Por supuesto, en ambas nubes, debemos considerar todos los equipos correspondientes de comunicación. La función del servidor es de ofrecer los servicios a los usuarios de la UDB-CS, los equipos RFID, perfectamente pueden usar como transportadora la señal WiFi, sin ocupar el ancho de banda completamente, sino que los tag mandan un pulso a los PA y estos se comunican al servidor indicando la ubicación de los equipos, el sistema puede ser tan complejo como se desee, tal es el caso que hasta el personal administrativo, de servicio y docentes se puede tener una trama; entonces el servidor reflejaría el código de equipo, el código de empleado y la ubicación. Aclaración, RFID, solamente utiliza una porción de la señal WiFi monitorear sus tag, RFID no está diseñado para servir como medio de comunicación a internet, los mismo sucede con Zigbee.

Nótese que se han agregado dos figuras más cañones y usuarios en ambos casos tienen tarjeta TAG, por lo que pueden ser monitoreados y el servidor tendría una trama de ubicación.

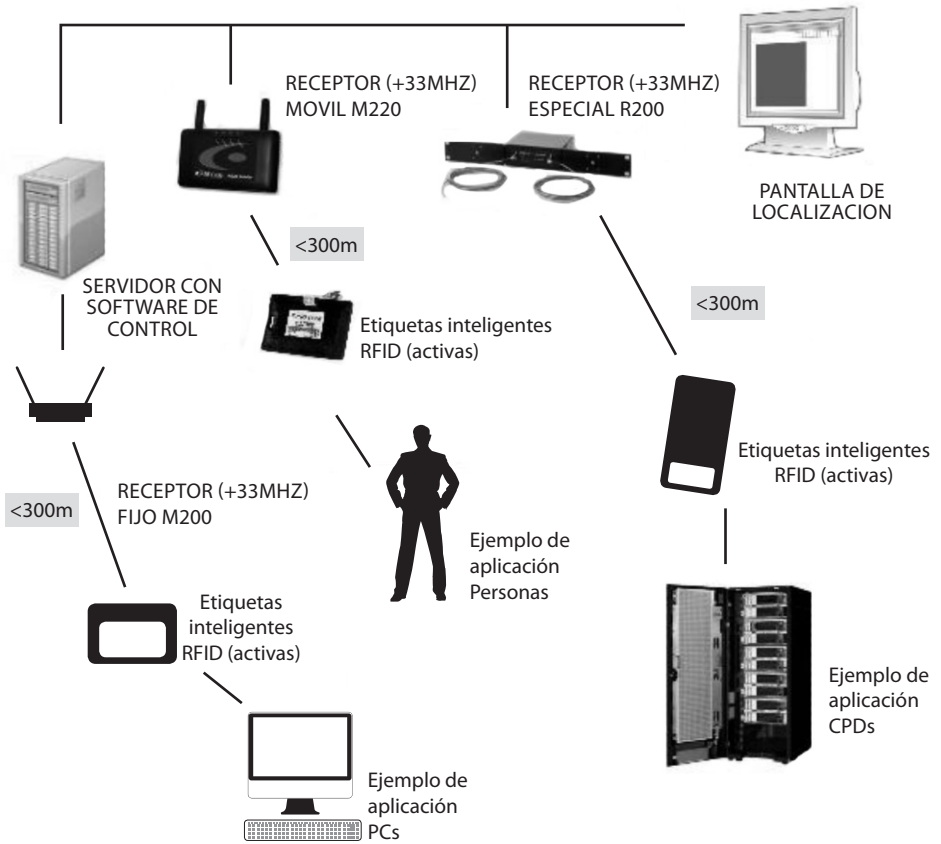


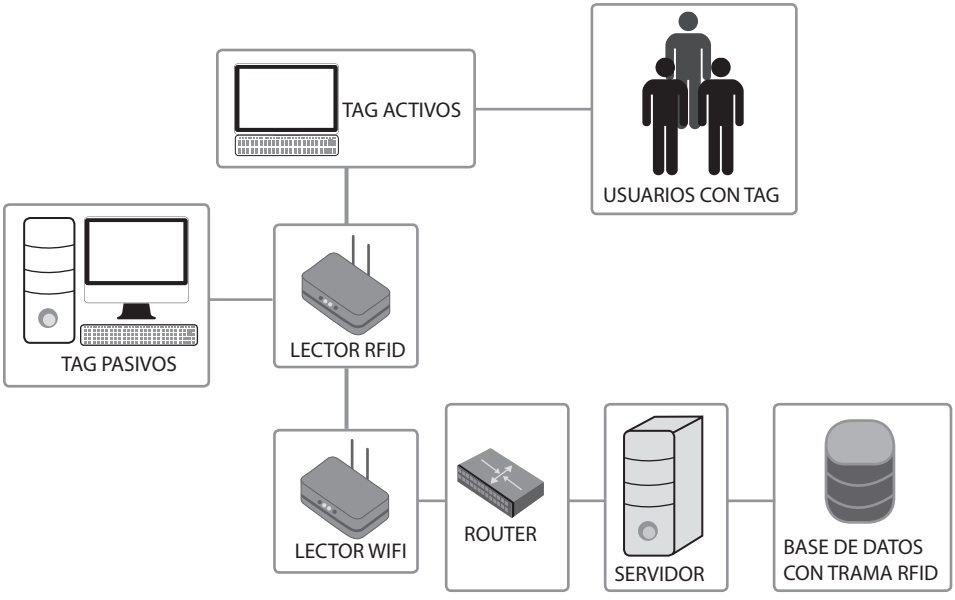
Figura 13. Tomada de vigiatech http://www.vigiatech.com/images/RFIDactiva.jpg

En ella podemos observar cómo interactúan los diferentes componentes RFID, interactuando para el monitoreo de equipos y personal.

La solución propuesta está en la parte Receptor Móvil M220, se podrían adquirir de 2 a 5 para que la vigilancia pueda monitorear los equipos móviles como las laptop, cañones entre otros, la etiqueta activa sería M100 tag, que puede ser asignada a los equipos e inclusive al personal, Con la solución M220 se suple un poco las áreas en las cuales no hay comunicación WiFi, ya que el lector portátil daría la ubicación, en este caso la vigilancia se comunicaría con caseta o portería indicando que uno de los equipos va rumbo a ellos y con esto tomar las medidas correspondientes. Pero en caseta se deben mantener las plumas abajo y los accesos peatonales cerrados para así poder registrar a los posibles infractores (ver anexo 7, para las características de los equipos propuestos).

En la configuración anterior, observamos como el equipo móvil con un tag manda una señal de radio frecuencia al lector este se conecta a la Red RFID, la cual está en comunicación con la Red WiFi, en el servidor de dicha red se lleva el control de trama de los equipos.

Se tendrían que colocar en los edificios de aulas estándar primera, segunda y tercera planta antenas receptoras para monitorear el desplazamiento de los equipos más personal, luego por medio de la WiFi, se transmiten los códigos correspondientes a la base de datos y con ello se mantiene un registro adecuado. No habría inversión en equipo WiFi, ya que se usaría el previamente instalado.



La Figura 14. Muestra una representación de conexión de equipos RFID con WiFi, desde tag activos como pasivos e incluso a los usuarios con tag. Estos son monitoreados por el lector RFID, luego usan como transportadora a la señal WiFi, en el servidor se llevará un control de la trama cada uno de los tag debe tener un código que lo identifica y la base de datos reconocerlo.

Se ha analizado la configuración RFID, pero es tiempo de colocar la configuración esquemática del ZigBee o protocolo 802.15.4

Recordemos que existen puntos donde no logra llegar la señal WiFi, por lo que nos veremos obligados a dar una solución diferente a la planteada.

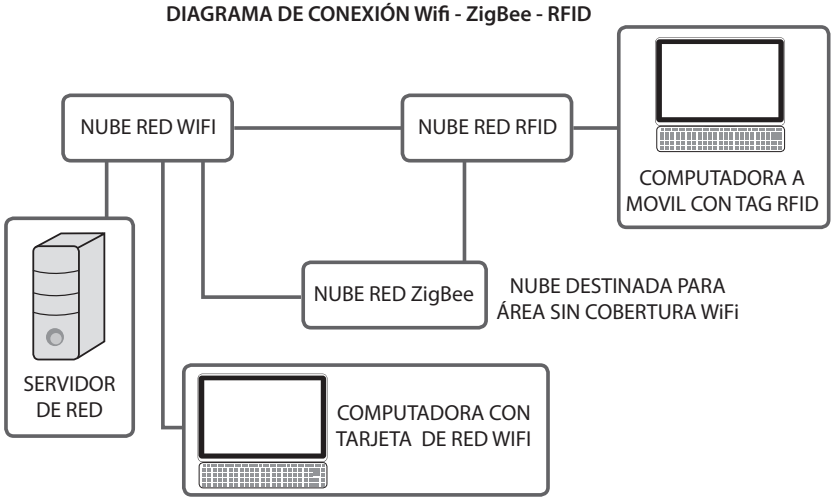


Figura 15.

En este caso, contamos con la cobertura especial, la Nube ZigBee, cubrirá las áreas donde la WiFi no llega, otra ventaja es que RFID, puede usar el ancho de banda de ZigBee para comunicarse con el servidor, de la misma forma el personal puede ser controlado por medio de su tag asignado.

Aclaración adicional, tanto RFID como ZigBee hacen uso de WiFi, pero hay un hibrido entre ambas tecnologías ZigBee y RFID, aun así sólo ZigBee, puede mantener una conexión propia.

Para dar una mejor explicación sobre, la solución propuesta en la siguiente imagen lo mostramos.

Imagen 4. Representación por nubes de cobertura WiFi y ZigBee

Primero identificaremos por color de nubes; las nubes amarillas representan a la transmisión WiFi, previamente instalada en la UDB-CS, la cual podemos observarla en los diferentes edificios de la universidad, con el agravante que la señal se pierde al trasladarse de un edificio a otro. Además entre más cerca estemos de los AP, mejor será la recepción de señal y entre más alejado estemos más potencia se requerirá para tener una conexión aceptable. Las señales WiFi, no pega en las pistas de vehículos y estacionamiento.

Segundo, las nubes rojas nos indican una conexión ZigBee con RFID, la finalidad, cuando los equipos móviles salgan de los edificios la señal WiFi se debilita y en cierto momento no hay señal disponible, en ese momento las antenas ZigBee, recibirán la señal de los tag, indicando la ubicación, otro punto importante, es dado el problema de las pistas donde no existe señal WiFi, el ZigBee lo suplirá manteniendo una conexión viable para el control de los equipos móviles; por lo que siempre se mantendrá un control de los equipos, ventaja del ZigBee es que este tiene una gran cobertura 1600 metros radiales, lo que cubre completamente el UDB-CS.

Como se logrará tener el control de los activos, en cada planta de los edificios de la UDB-CS, se colocarían tres antenas fijas de RFID que se comunicarían con los AP WiFi, con esto se tendrá una triangulación para la ubicación exacta el tag activo mandaría su señal a las antenas y estas pasarían la traza de la señal al software del monitoreo ver anexo 7; en el caso que el equipo móvil no esté dentro de la cobertura WiFi, las antenas Zigbee serían las encargadas de monitorearlos y con ello no perderíamos la traza. Todo esto se logra nuevamente con la red WiFi.

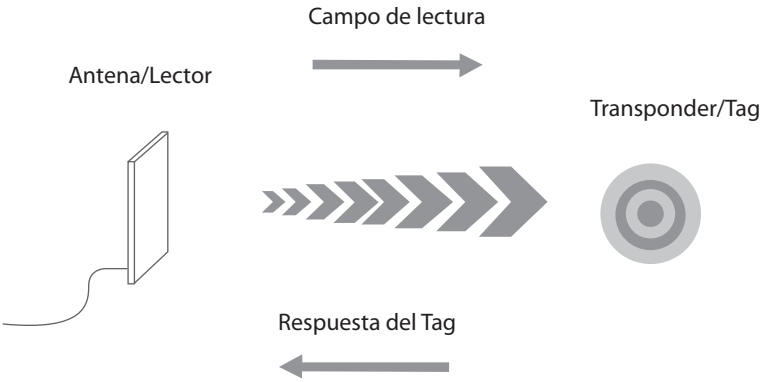


Figura 16. Representación de funcionamiento de una señal RFID.

Fachada de la nueva biblioteca, en la entrada se colocaría un AP de RFID controlando la señal de equipos móviles propiedad de la Universidad tales como: Laptops, cañones, retroproyectores.

Imagen 6. Edificio de Aula Estándar "C".

Edificio de Aulas Estándar "C, es de tres niveles en el primero hay aulas de Diseño Gráfico y oficinas de la Facultad de Economía con oficinas de la Facultad de Estudios Tecnológicos, del segundo nivel al tercer nivel son Aulas, se propone colocar en cada piso tres antenas lectoras RFID fijas en techo para controlar en cada nivel los equipos móviles, ya mencionados. Las Aulas Estándar "A" y "B" son iguales a la descrita.

Análisis de costos

Cotización para equipos RFID

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	PRECIO TOTAL
27	M200, equipo para lectura fija se colocarían tres en cada planta de los edificios del campus incluye cafetería, queda a discreción de las autoridades	$180.00	$4,860.00
1	Impresoras para tag de alto rendimiento industrial	$5,764.85	$5,764.85
15	Etiqueta RFID rígida grande UHF, encapsulado para entornos adversos, excelente rendimiento UHF, disponible para Gen 2 y silicón ISO 18000 -6B Etiqueta IT32A Gen 2 ID, rendimiento superior en múltiples superficies, reutilizable	$35.00	$525.00
2	M220 Lector móvil alcance de 70 Mts. Puede ser usado por la vigilancia de a pie o en bicicleta y con ello suplir la comunicación en puntos ciegos.	$990.00	$1,980.00
TOTAL INVERSIÓN			$16,099.85

Cotización para equipo ZigBee

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	PRECIO TOTAL
3	DRF2619A, antenas de 1600 mts radiales capaz de cubrir el Campus de la universidad	$40.30	$120.90
3	XBee Pro 60mW Wire Antenna - Series 1 (802.15.4)	37.95	113.85
TOTAL			$234.75

Los equipos RFID, pueden configurarse para comunicarse con las antenas ZigBee, es por ello que no se solicita otro equipo, el total de la inversión sería $ 16,334.16. Dólares americanos. La inversión es un poco alta pero se creería que se recupera en un corto tiempo, si se le cobra a cada estudiante un costo adicional al momento de adquirir el carné. Haciendo números.

Carné $ 35.0 dólares americanos multiplicado por la cantidad de alumnos inscritos 4000 esto nos da un total de $ 157,500.00 dólares.

Por lo que la inversión se recuperaría en el primer año de funcionamiento.

Es difícil hacer una comparación o análisis sobre los bienes móviles hurtados en costo monetario total y la inversión que se realizaría con respecto a los equipos RFID y ZigBee que se instalaren, el motivo es por confidencialidad.

En el país hay empresas que comercialicen equipos RFID y ZigBee tales como:

El Salvador
http://www.itrsal.com.

América
http://www.quiminet.com/sh3/sh_RsDFbcBuaasdRsDF.htm
http://www.logisticamx.enfasis.com/notas/4585-guia-practica-proveedores-tecnologia-rfid
http://www.mclogistica.com/tecnologias/identificacion-por-radio-frecuencia-rfid/

Pero en Estados Unidos. Existen empresas que comercializan dichos equipos.

Europa
http://www.dipolerfid.es/
http://www.quiminet.com/shr/es/shenzhen-rich-electronics-3711402349.htm

Conclusiones

Al estudiar la manera como se asignaban los equipos móviles de bodega hasta los salones de clases o salones de reuniones se tenía riesgos que el docente o encargado no estuviere en el lugar especificado en la orden de uso de los equipos, que por descuido el encargado olvidará los equipos y estos fueren hurtados. Por lo que, el riesgo latente del momento es real.

1-El análisis realizado con VISTUMBLER, sobre la potencia de la señal en los diferentes edificios y áreas libres del campus se observa que las señales son débiles a medida que nos alejamos de los edificios, por lo que se necesita mayor potencia para cubrir áreas mayores a 20 metros, incluso tomando en consideración los obstáculos que atenúan la señal. Significa que los equipos móviles interactuando con WiFi y RFID no pueden cubrir traslado de edificios con su trazabilidad.

2-RFID permitiría controlar la movilidad de los bienes de la Universidad Don Bosco – Campus Soyapango (UDB-CS), llevando para ello una trazabilidad de la ubicación donde este se encuentre, de igual manera se agrega un plus y es que se puede asignar a las tarjetas de visitas tag activos, para controlar adonde se dirigen y si ha ido al lugar indicado, con ellos se mantendría un control más efectivo.

3-Aparte de la solución ofrecida con ZigBee, RFID, suple la necesidad de los puntos ciegos utilizando para ello lectores móviles con alcance de 70 metros los cuales pueden ser usados por la vigilancia y monitorear las pistas de parqueo.

4-Se ha explicado, cómo funciona un sistema ZigBee (Protocolo 802.4.15) para realizar una comparación de tecnologías de comunicación y con ello tener una idea más clara de la viabilidad de conexión, por lo que se determina que el

sistema ón WiFi, que está actualmente en uso en la UDB-CS no es adecuado para poder monitorear equipos móviles, ya que las potencias presentadas en la señal no son las adecuadas, con el agravante de que, si uno de los equipos fuere sustraído y sacado de las instalaciones no habría forma de detectarlo en las casetas tanto de vehículos como peatonales, habiendo para ello muchos puntos ciegos. En consecuencia a lo anterior, se propone que un sistema ZigBee es el más adecuado para ello, cuenta con un rango de acción en señal de 1600 metros radiales, con tres antenas principales se puede cubrir el campus de la universidad y mantener un control efectivo de los equipos. Inclusive cubriría teóricamente hasta áreas que están siendo radiadas por WiFi.

5-En el caso que las autoridades de la universidad se interesen en el estudio realizado para una futura implementación de un sistema de monitoreo, recomendaría profundizar más en el estudio para que se tengan mejores elementos de decisión y con ello proteger el campus e inclusive la Ciudadela.

Bibliografía

[1] Mbps: Mega bits por segundo, Soyer, Laurence, Wi-Fi: Instalar una red inalámbrica en casa, Ediciones ENI Po Ferrocarriles Catalanes, 97-117, 2gndo. pl.of.18 08940-Cornella de Llobregat Barcelona – España. Agosto 2005.

[2] IEEE 802.11 Estándar que fue ratificado en julio de 1997 funciona en la banda de 2,4GHz con velocidad de transmisión máxima de 2Mbps, ha sido el más utilizado en las redes WLAN, F. Andreu, WLAN Fundamentos y aplicaciones de seguridad, Marcombo, S.A de C.V 2006, Página 22.

[3] WLAN, F. Andreu, WLAN Fundamentos y aplicaciones de seguridad, Marcombo, S.A de C.V, 2006, Pagina 23.

Vidri. S.I, (2011-2012), ZigBee y sus aplicaciones, Recuperado de: http://www.dea.icai.upco.es/sadot/Comunicaciones/avanzadas/Zigbee%20y%20sus%20aplicaciones.pdf

Marca: DTK, Número de Modelo: DRF2617A Place of Origin: China (Mainland)(2007), Recuperado de: http://es.aliexpress.com/item/ZigBee-Module-RS232-to-ZigBee-1-6-km-transfer-ZigBee2007/494931741.html

Marca: shuncom, Place of Origin: China (Mainland), Recuperado de:
http://es.aliexpress.com/item/2-4G-zigbee-module-SZ02-232-2k/564961265.html

DEPARTAMENTO DE CIENCIA Y TECNOLOGÍAUNIVERSIDAD NACIONAL DE QUILMES, Recuperado de: http://iaci.unq.edu.ar/materias/telecomunicaciones/archivos/2008/Unidades%20de%20medidas%20en%20Telecomunicaciones.pdf

Cortes.C. (2009), Diseño de un protocolo de identificaciónpor radiofrecuencia (RFID) propietario para una aplicación específica, Recuperado de:
http://ingenieriayApplicationuniversidad.javeriana.edu.co/Vol13nr2Protocolo.pdf

Diagnani J.P. (2011), Anàlisis de protocolo zigbee, Recuperado de:
http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Dignanni_Jorge_Pablo.pdf

Active RFID Tracking - RF*IDI, LLC, Recuperado de:
http://www.activerfidtracking.com/rfidi/Hardware.aspx?catId=c13

Motorola Solutions, Recuperado de:
http://www.motorolasolutions.com/XL-ES/Productos+y+Servicios+para+Empresas/RFID

Editorial
Universidad Don Bosco

Raúl Martínez Rivas es Ingeniero en Ciencias de la Computación por la Universidad Politécnica y Máster en Arquitectura de Software por la Universidad Don Bosco. Catedrático de la Escuela de Ingeniería en Ciencias de la Computación de la Universidad Don Bosco.