UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERÍA EN COMPUTACIÓN

Con estudios incorporados a la
Universidad Nacional Autónoma de México
CLAVE: 8793-16

"TECNOLOGÍA INALÁMBRICA BLUETOOTH"

TESIS

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA:

RICARDO GARCÍA ORTEGA

Asesor: Ing. Carlos Alfonso Hernández Villanueva

Celaya, Gto. **Septiembre del 2007**

DEDICATORIAS

A mi esposa:

Que a cada instante de nuestras vidas ha impulsado arduamente los logros que hemos conseguido juntos y este es el más importante en este momento; porque sin ti simple y sencillamente no estaría escribiendo estas líneas. Gracias mi “chinita hermosa”.

A mis padres:

Porque gracias a ustedes con su esfuerzo y sacrificio me dieron la oportunidad de estudiar la Ingeniería en Computación que hoy culmino. Les puedo decir orgullosamente que cumplieron cabalmente con el reto más importante y significativo para un padre: brindar la educación a sus hijos.

A mí amado “Gigante de Hierro”

Porque a pesar de tu corta edad me has enseñado que todo se puede lograr en esta vida, que los obstáculos no existen y que el trabajo constante y férreo es el arma más poderosa para salir adelante.

Gracias “Mí Ricardito hermoso”

“Tecnología inalámbrica Bluetooth”

INTRODUCCIÓN

CAPÍTULO I. INTRODUCCIÓN A LA TECNOLOGÍA BLUETOOTH

CAPÍTULO II. ARQUITECTURA Y FUNCIONAMIENTO BLUETOOTH

CAPÍTULO III. BLUETOOTH Y LAS COMUNICACIONES INALÁMBRICAS DE TERCERA GENERACIÓN

TECNOLOGÍA

INALÁMBRICA BLUETOOTH

INTRODUCCIÓN

La tecnología inalámbrica Bluetooth se ha convertido en una especificación global de carácter tecnológico para el establecimiento de comunicaciones inalámbricas entre dispositivos portátiles, equipos de escritorio y periféricos.

Entre las diferentes actividades que esta tecnología nos permite realizar a los usuarios podríamos resaltar el intercambio de datos y la sincronización de archivos sin necesidad de conectar por cable los dispositivos. Además es pertinente mencionar que el enlace inalámbrico tiene un radio de acción de 10 metros, por lo tanto los usuarios tienen más movilidad que nunca. Al eliminar los cables, el entorno de trabajo también parece más cómodo y atractivo.

Esta tecnología también puede emplearse para realizar conexiones de datos inalámbricas a redes de área local convencionales, a través de un punto de acceso equipado con un transceptor radio Bluetooth que está concectado a la LAN, incluyendo impresoras, servidores de bases de datos y conexiones a internet. Por ejemplo, también si uno desea puede escribir la respuesta a un correo electrónico en su dispositivo de mano y decirle al dispositivo que establezca una conexión a internet a través del teléfono móvil, imprimir una copia en una impresora cercana, todo ello mientras uno se dirige hacia la sala de reuniones para mantener una exposición de trabajo.

El protocolo de banda base Bluetooth es una combinación de conmutación de paquetes y de circuitos, lo que lo hace adecuado tanto para voz como para datos. Por ejemplo en lugar de utilizar el teléfono celular mientras conduce, el chofer puede llevar puesto un audífono para responder una llamada e inicializar una conversación sin ni siquiera sacar su teléfono de su maletín.

Con la tecnología Bluetooth realizar una conexión es tan fácil como encender el dispositivo. No hay necesidad de que el usuario apriete un botón para iniciar un proceso. De hecho, una de las ventajas principales de la tecnología inalámbrica Bluetooth es que no necesita configuración, siempre está activa, ejecutándose en segundo plano. Los dispositivos Bluetooth exploran su entorno en busca de otros dispositivos Bluetooth y, cuando dos dispositivos entran dentro del rango mutuo de cobertura, empiezan a intercambiar mensajes para conocer cuáles son las capacidades de cada uno, establecer conexiones, y en caso necesario, disponer los mecanismos de seguridad para proteger los datos confidenciales durante la transmisión.

En esta tesis que tiene por nombre **“Tecnología inalámbrica Bluetooth”** quiero dar a conocer el entusiasmo sin precedentes que ha despertado dicha tecnología en todos los sectores de la industria informática y de comunicaciones. Es por eso que la tecnología Bluetooth es integrada en cientos de millones de teléfonos móviles, equipos informáticos de escritorio y muchos otros dispositivos electrónicos. Esta tesis explica a los lectores las ventajas que la tecnología inalámbrica Bluetooth ofrece a los usuarios para una gran

variedad de aplicaciones, y explica los detalles fundamentales de operación de la tecnología y su relación con la infraestructura inalámbrica global emergente de tercera generación.

En el **primer capítulo** se adentra al lector con una breve y clara introducción de la tecnología inalámbrica Bluetooth para darle un panorama completo y general para su mayor entendimiento y comprensión.

Después de conocer los conceptos básicos o generales continuamos con el **segundo capítulo**, se analiza y se hace una comparación de la tecnología inalámbrica Bluetooth con otras tecnologías inalámbricas como lo son los rayos infrarrojos y las redes inalámbricas.

En el **tercer capítulo**, se habla de las comunicaciones celulares de tercera generación ya que tienen una amplia relación de trabajo con la tecnología Bluetooth y por ello se describe ampliamente el desarrollo de las distintas generaciones de telefonía celular hasta hoy en día.

Cuarto capítulo menciona la seguridad de la tecnología inalámbrica Bluetooth ya que es un tema indiscutiblemente interesante e importante porque nos brinda la seguridad de tener nuestras transmisiones siempre confiables y con la certeza de que nadie nos esté pirateando nuestra información.

CAPÍTULO I. INTRODUCCIÓN A LA TECNOLOGÍA BLUETOOTH

1.1 ¿QUÉ ES BLUETOOTH?

Bluetooth es una tecnología inalámbrica que facilita la computación móvil; es decir, favorece la comunicación entre dispositivos y la conexión a Internet a altas velocidades, sin el uso de cables. Además, hace posible la sincronización de datos de computadoras móviles, teléfonos celulares y manejadores de dispositivos (figura 1.1).

Figura 1.1 Dispositivos móviles Fuente: www.google.com

La tecnología Bluetooth tiene la ventaja de que es de pequeña escala, bajo costo y se caracteriza por usar enlaces de radio de corto alcance entre móviles y otros dispositivos, como teléfonos celulares, puntos de accesos de red (access points) y computadoras. Esta tecnología funciona en la banda de 2.4 GHz, tiene la capacidad de atravesar paredes y maletas, lo cual la hace ideal tanto para el trabajo móvil, como el trabajo en oficinas.

La tecnología inalámbrica Bluetooth por ser una combinación de conmutación[1] de circuitos y de paquetes, es altamente apropiada tanto para voz como para datos.

Esta tecnología se implementa en transmisores de corto alcance pequeños y de bajo costo en los dispositivos móviles disponibles hoy en día, ya sea integrada directamente en tarjetas de expansión existentes, o añadida mediante dispositivos adaptadores, como una tarjeta PC-card[2] insertada en una portátil. Por tal motivo, esto puede hacer que los dispositivos que utilicen la especificación Bluetooth sean la tecnología más barata de implementar.

No es necesario comprar nuevos dispositivos para sacar partido de la tecnología inalámbrica Bluetooth. Por ejemplo, los que hayan comprado un Visor de Handspring (un dispositivo muy parecido al Palm Pilot, pero más barato y funcional) podrán insertar un módulo llamado Blue-Connect. El módulo Blue-Connect transmite aplicaciones

[1] "Según el diccionario ilustrado océano conmutar significa cambiar o permutar una cosa por otra."
[2] Las tarjetas PC Card de expansión son del tamaño de una tarjeta de crédito que se utilizan para agregar no sólo el adaptador o controlador par un dispositivo periférico, sino todo el dispositivo mismo.

de Visor a Visor o de Visor a un PC de escritorio o una portátil, con un esquema de sincronización llamado Blue-Share. También puede transmitir datos de la agenda de direcciones y transferir imágenes entre el Visor y cámaras digitales.

Como podemos apreciar, la tendencia de la tecnología Bluetooth (figuras 1.2) es hacer la vida más fácil de las personas que interactúan con dispositivos periféricos y con la enorme ventaja de abaratar los costos en comparación con tecnologías similares que más adelante se mencionarán. Una ventaja más de la tecnología Bluetooth es que no por el hecho de ser novedosa se tendrá que desechar los dispositivos actuales con los que estamos trabajando, sino solamente con agregarle una tarjeta o módulo; con ello, los equipos actuales trabajarán de manera conjunta con la tecnología, sin desembolsar grandes cantidades de dinero en inversiones de nuevos equipos que cuenten con la tecnología desde su fabricación.

Figura 1.2 Tendencia Bluetooth Fuente: www.google.com

1.1.1 ¿CÓMO SURGIÓ EL ESTÁNDAR?

En el año de 1994 surgió la idea de Ericsson Mobile Comunications de investigar la posibilidad de crear un dispositivo de bajo costo, el cual consistía en una interfaz de radio que sirviera para comunicar diversos dispositivos; la idea era hacerlo basado en un estándar estricto para que su uso se popularizara y así diversos fabricantes pudieran desarrollar dispositivos que lo utilizaran. Con el fin de conseguir y promocionar un único estándar mundial, Ericsson se acercó a otros productores de dispositivos portátiles a principios de 1997.

En 1998, un grupo de industrias líderes en computadoras y telecomunicaciones, incluyendo Intel, IBM, Toshiba, Ericsson y Nokia, estuvieron desarrollando dicho dispositivo. Para asegurar que esta tecnología esté implementada con un empalme perfecto en un diverso rango de dispositivos, esos líderes formaron un grupo de intereses especiales (Special Interests Group - SIG). El SIG consiguió rápidamente más miembros, como las compañías 3Com, Axis Comunication, Compaq, Dell, Motorola, Qualcomm y Xircom.

En la actualidad, las compañías que han firmado este acuerdo son aproximadamente unas 2500. Para mantener la calidad y asegurar la interoperatividad, los productos Bluetooth tienen que garantizar su compatibilidad antes de que puedan ser comercializados.

La tecnología Bluetooth, como se observa, está ampliamente respaldada por los gigantescos emporios que ven en ella un gran futuro; de esta manera se facilita su implementación en los productos que estas grandes compañías fabrican y por tal motivo se espera que

la tecnología alcance todavía más, un gran número de socios, contribuyendo a ello a un potencial crecimiento y así convertirse en el número uno de su ramo. Por esta razón debemos confiar ampliamente en esta innovación tecnológica, ya que nos garantiza una seguridad y un respaldo enorme puesto que las compañías interesadas en ella son lideres comerciales en el mundo.

1.2 ¿DE DÓNDE VIENE EL NOMBRE?

Los ingenieros de Ericsson denominaron Bluetooth a la nueva tecnología inalámbrica para venerar a un rey vikingo danés del siglo X. Harald Bluetooth fue famoso por sus habilidades comunicativas y reinó desde 940 a 985 y se le atribuye no sólo la unificación de ese país, sino también la adopción del cristianismo.

En esa época los daneses vivían en pequeñas comunidades bajo la autoridad de jefes locales, algunos de los cuales aterrorizaron las ciudades costeras de Europa con sus incursiones piratas vikingas para conseguir esclavos y botín. Durante siglos, los daneses habían venerado a los dioses Thor y Odin. A medida que el cristianismo dominaba Europa, la lucha entre cristianos y paganos se extendió por las áreas ocupadas por los daneses.

La historia comenta que Harald era hijo del rey Gorm el Viejo de Dinamarca y de Thyra (o Tyra), que se decía que era hija de un noble inglés. Cuando llevaba unos 25 años de reinado, el sacerdote alemán Poppos impresionó a Harald sujetando una pieza de metal al rojo vivo con sus manos desnudas sin producirse ninguna herida. Poppos

explicó que su Fe en Dios le protegía, lo que convenció a Harald de los poderes del cristianismo. La aceptación del cristianismo por el rey Harald y su subsiguiente bautizo hizo mucho para aliviar las luchas religiosas en Dinamarca.

Los objetivos de la tecnología inalámbrica Bluetooth son también la unificación y la armonía: específicamente, el permitir a diferentes dispositivos que se comuniquen a través de un estándar ampliamente aceptado para la conectividad inalámbrica. Resulta un tanto chusco, pero así es como el personal de marketing de Ericsson explica la selección del nombre “Bluetooth”.

1.3 ¿QUÉ SE PUEDE HACER CON BLUETOOTH?

La tecnología Bluetooth le permite conectarse a una amplia variedad de dispositivos informáticos y de telecomunicaciones de una forma sencilla y simple, sin necesidad de comprar, llevar o conectar cable.

Ofrece oportunidades de conexiones rápidas y posibilita las conexiones automáticas entre dispositivos.

Las figuras siguientes (ver figuras 1.3) muestran un claro ejemplo real de lo que podemos llegar a realizar al momento de comprar dispositivos electrónicos que lleven en su interior un chip bluetooth, lo cual es de gran ayuda en nuestras vidas diarias porque nos olvidamos por completo de los cables.

Figura 1.3 ¿Qué se puede llegar hacer con Bluetooth? Fuente: www.google.com

1.3.1 ESCANEADO DE TARJETAS

Con un escáner de tarjetas que utilice la tecnología Bluetooth, se puede escánear tarjetas en la propia computadora de uno, o en cualquier otra computadora que se encuentre dentro del rango de 10 metros, sin tener que pasar por la molestia de conectar, desconectar y volver a conectar cables entre los equipos.

1.3.2 SINCRONIZACIÓN DE DATOS

Una innovación que pueden realizar los dispositivos Bluetooth es el envío de mensajes a dispositivos en modo de reposo. Por ejemplo, cuando un teléfono móvil recibe un mensaje, puede enviarlo a una computadora portátil, incluso aunque esta última se halle dentro en una maleta. Por cierto, esta tecnología también puede emplearse para sincronizar datos entre dispositivos.

La sincronización automática resulta ser un ahorro de tiempo. Cuando se haya acabado de agregar información a la computadora de mano en casa; después, todo lo que se tiene que hacer es ir a trabajar a la oficina para cargar esos archivos en la PC de escritorio.

Cuando uno se tenga que retirar de la oficina, cualquier archivo nuevo que se haya agregado a la PC de escritorio se copiara automáticamente a la computadora de mano. Cuando lleguemos a casa en el transcurso de la noche, por ejemplo, se cargará automáticamente la nueva información en la portátil tan pronto como los dos dispositivos entren dentro del radio de acción, de esta manera no se tiene que hacer nada: el enlace simplemente se produce de manera automática.

Con la sincronización automática, ya no hay ninguna confusión sobre qué archivo está en qué equipo: la especificación Bluetooth garantiza que tenga la información más actualizada, independientemente de qué dispositivo utilice en su momento dado.

1.3.3 IMPRESIÓN

Con la tecnología inalámbrica Bluetooth, una cámara digital podría enviar una fotografía directamente a la impresora, así también, segundos después de que se haya tomado una fotografía, la cámara digital podría enviar una imagen a un dispositivo electrónico de bolsillo, el cual luego podría enviar la foto adjunta a un correo electrónico.

1.3.4 SISTEMAS INCORPORADOS EN AUTOMÓVILES

La especificación Bluetooth permite a innumerables dispositivos digitales compartir información en forma inalámbrica dentro de un automóvil: desde teléfonos celulares a computadoras de mano y otros dispositivos.

Entre las compañías que ofrecen esos sistemas se halla Johnson Conttrols. El dispositivo TravelNote Connect de esa compañía prácticamente es una grabadora digital TravelNote pero modificada que integra tecnología inalámbrica Bluetooth. TravelNote es un dispositivo digital de grabación/reproducción que se puede integrar a un cuadro de control. Permite a la persona que ocupe el asiento delantero grabar, guardar y reproducir mensajes recordatorios. Además, también al agregar un componente con tecnología inalámbrica Bluetooth, el dispositivo puede realizar otras actividades tales como conseguir un número de teléfono del teléfono celular y marcarlo automáticamente, y así el conductor no tenga que apartar

sus manos del volante. Cuando se establece la conexión, el componente Bluetooth crea un enlace inalámbrico de voz con el teléfono celular, proporcionando la capacidad de manos libres al hablante.

Este producto y otros similares de otros fabricantes tienen la capacidad de hacer de cada teléfono celular un teléfono con manos libres, sin complicadas modificaciones o costosas instalaciones en el interior de un vehículo. Como todos los dispositivos que utilizan la tecnología inalámbrica Bluetooth pueden hablar con otros dispositivos igualmente equipados, se pueden mezclar y emparejar productos para su uso en el vehículo, independientemente del modelo, marca o fabricante.

Un ejemplo de lo dicho anteriormente es que cada día son más los fabricantes de automóviles que están incluyendo como equipamiento de serie o bien como opción, un sistema de manos libres Bluetooth para el teléfono. Prueba de ello es el nuevo Audi A8, el cual salió a la venta con la opción de kit manos libres Bluetooth.

Audi ha seguido los pasos de otros fabricantes que ya incluyeron esta opción en su día, como BMW, Chrysler, Mercedes o más recientemente Peugeot. Este hecho, no hace sino que reafirmar la apuesta de la industria automovilística por la tecnología Bluetooth como método de interconexión de sistemas del vehículo con otros dispositivos personales, como ahora ocurre en el caso de la telefonía, pero que en el futuro se ampliará a otras posibilidades.

1.3.5 LIBROS ELECTRÓNICOS

Ahora que los libros electrónicos se están poniendo de moda, puede adquirir títulos de libros en la web, en librerías en línea, y descargarlos a una computadora de escritorio o a una portátil. Básicamente, la computadora se convierte en una biblioteca electrónica en la que se pueden seleccionar volúmenes específicos. Por medio de un programa biblioteca que gestiona los títulos en la computadora se pueden transferir cualquier volumen electrónico (así como documentos) a un dispositivo especial de lectura llamado libro electrónico o “ebook”, el cual se conecta a una estación de acoplamiento enlazada por cable a la computadora. El ebook es un dispositivo portátil alimentado por baterías que pesan tan sólo 627 gramos. Tiene una iluminación trasera blanca para facilitar la lectura de los textos. Cuando se mejoren estos ebooks con la tecnología inalámbrica Bluetooth, se podrá transferir títulos preseleccionados entre los dispositivos simplemente colocando el ebook dentro del alcance de la computadora en la que esté su biblioteca.

La tecnología inalámbrica Bluetooth, como ya es sabido, proporciona una gran cantidad de beneficios para los usuarios finales, ya que la idea central es la de facilitar cada día más la vida del ser humano, teniendo como característica primordial el eliminar los cables (ver ejemplos de figuras 1.4 y 1.5), los cuales nos permiten interactuar con los diferentes componentes electrónicos. Con esta característica principal uno como usuario puede realizar un sinnúmero de actividades ahorrando con ello esfuerzo, tiempo, dinero. Pero, sobretodo, lo maravilloso es que se puede emplear en cualquier lugar

que uno desee sin tener que preocuparse de llevar con uno los cables, sino sólo centrarse en la PC y el dispositivo con el que se vaya a interactuar. Por ejemplo, un ejecutivo que tenga que exponer una conferencia sólo tendrá que llevar su laptop a la sala de exposición y ver que cuente con una pantalla o con un proyector y con la interacción de estos dos dispositivos podrá realizar su conferencia de una manera fluida sin tener que conectar un solo cable.

Ahora, también el tener una PC en casa, implica tener una mesa de trabajo llena de cables, los cuales llegan a formar en ocasiones una "gran madeja" que molesta porque luego no se distingue qué cable pertenece a cada dispositivo. Con la llegada de la tecnología Bluetooth esta gran madeja de cables desaparecerá; el mouse, la impresora, el scanner, etc., ya no dependerán de un cable para su funcionamiento sino que funcionarán de manera inalámbrica ahorrando espacio.

RELOJES BLUETOOTH(SONY ERICSSON)

"Equipados de conectividad bluetooth y la posibilidad de aceptar o rechazar llamadas desde el equipo, y lo más interesante controlar el reproductor de música del teléfono. "

Figura 1.4 Ejemplos de conectividad Bluetooth Fuente: www.google.com

H5 MINIBLUE

"El H5 Miniblue es un headphone tecnológicamente sorprendente, tanto el auricular como el micrófono son in-ear, esto funciona porque toma la voz desde el canal auditivo, algo que Motorola asegura que produce conversaciones claras y sin interferencias "

Figura 1.5 Ejemplos de conectividad Bluetooth Fuente: www.google.com

CAPÍTULO II. ARQUITECTURA Y FUNCIONAMIENTO DE BLUETOOTH

2.1 FUNCIONAMIENTO DE INFRARROJOS

Esta tecnología, basada en rayos luminosos que se mueven en el espectro infrarrojo, es una de las más “veteranas” en el ramo informático de la comunicación sin cables. Por ello, hace tiempo que podemos encontrar gran cantidad de periféricos que la emplean para comunicarse con el ordenador e intercambiar información. Es la misma técnica utilizada por los controles remotos de nuestros televisores.

IrDA (*The Infrared Data Association*) es una organización fundada en 1993 con el objetivo de crear el hardware y el software apropiado para hacer posible las comunicaciones inalámbricas mediante luz infrarroja.

Actualmente encontramos que esta tecnología es implementada en la práctica, en la mayoría de los ordenadores portátiles, móviles, cámaras digitales y otros cientos de dispositivos. Esta tecnología se divide en dos aplicaciones para cubrir todas las necesidades del mercado, estas dos aplicaciones distintas son: IrDA-Data e IrDA-Control.

La primera de ellas, IrDA-Data, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y

los 4 Mbps. Esta oscilación depende del tipo de transmisión (síncrona o asíncrona), la calidad del controlador que maneja los puertos infrarrojos, el tipo de dispositivo, y por supuesto, la distancia que separa ambos extremos. De hecho, éste es uno de los puntos más problemáticos, ya que aunque la distancia entre emisor y receptor puede alcanzar los 2 metros, no se recomienda superar uno. Un ejemplo claro son los puertos de bajo consumo instalados en móviles y pequeños PDAs, cuya área de acción se reduce a no más de 30 cm. En cualquiera de los casos, debemos de colocar los artículos en un ángulo máximo de 30 grados y contar con un espacio libre de obstáculos entre ellos.

Para que la transmisión de los productos IrDA-Data sea posible, se deben tomar en cuenta tres protocolos básicos: PHY (*Physical Signaling Layer*), este protocolo establece la distancia máxima, la velocidad de transmisión y la manera en que la información se transmitirá; IrLAP (*Link Access Protocol*), proporciona la conexión del dispositivo facilitando así la comunicación además de marcar los procedimientos para la búsqueda e identificación de otros aparatos que se encuentren preparados para comunicarse, y por último, IrLMP (Link Management Protocol), permite la multiplexación de la capa IrLAP, esto es, admite múltiples canales sobre una conexión IrLAP. Además de estos tres protocolos, existen otros siete que ofrecen funcionalidades extra para acceder a redes de área local, teléfonos móviles o cámaras digitales.

El otro tipo de puerto infrarrojo, el IrDA-Control se ha diseñado para conectar periféricos de control como teclados, ratones, dispositivos

apuntadores o joysticks a una estación fija, por ejemplo una PC, una consola de videojuegos o un televisor. Sin embargo, las diferencias son notables, ya que la distancia máxima se amplía hasta garantizar un mínimo de 5 metros. La velocidad de transmisión, algo que no es crítico para el tipo de productos al que se dirige, alcanza 75 Kbps. Y como ocurre en el caso anterior, para que esto sea posible, cuenta con tres protocolos que establecen la comunicación: PHY (*Physical Signaling Layer*), este protocolo vuelve a marcar la velocidad y distancia de transmisión, mientras que MAC (*Media Access Control*) es el responsable de proporcionar soporte hasta ocho dispositivos simultáneos conectados al mismo receptor; finalmente, nos encontramos con el LLC (Logical Link Control), que realiza ciertas funciones de seguridad y retransmisiones en caso de que el envío de información haya fracasado.

2.1.1 CARACTERÍSTICA DE FUNCIONAMIENTO DE LOS INFRARROJOS

Tabla 2.1 Características de los infrarrojos

Característica/Función	Funcionamiento
Tipo de conexión	Infrarrojos, haz estrecho (ángulo de grados o menos).
Espectro	Óptico, 850 nanómetros (nm)
Potencia de transmisión	100 milivatios (mW)

Velocidad de transferen de datos	Hasta 16 Mbps usando VFIR (Very Fast Infrared, infrarrojos muy rápidos)
Alcance	Hasta 1 metro
Dispositivos soportados	Dos (2)
Canales de voz	Uno (1)
Seguridad de los datos	El corto alcance y estrecho ángulo de Haz de infrarrojos ofrecen una forma simple de seguridad; por lo demás, no hay funciones de seguridad el nivel de enlace.
Direccionamiento	Cada dispositivo tiene un identificador físico de 32 bits que se utiliza para establecer una conexión con otro dispositivo.

Como se puede apreciar, esto de las comunicaciones inalámbricas ya no es algo nuevo en el sector de la electrónica, sin embargo ha ido evolucionando notablemente. Uno de los pioneros en este aspecto es la comunicación inalámbrica vía rayos infrarrojos, los cuales, como se vió en este apartado, buscan la misma funcionalidad que la tecnología inalámbrica Bluetooth.

Cabe mencionar que el funcionamiento de estos rayos infrarrojos lo podemos apreciar día con día en nuestros hogares, un ejemplo claro es el control remoto de la televisión el cual funciona con esta tecnología. Como se sabe, el control emite un haz, de luz que es interceptado por la televisión, la cual activa la señal que se le indica del control. Haciendo hincapié sobre una comparación entre Bluetooth y los infrarrojos, es que estos últimos no tienen la facilidad de traspasar objetos, necesitan siempre un camino sin obstáculos para que puedan funcionar. Si al control remoto de la televisión le ponemos la palma de nuestra mano, ocasionará que no se emita el haz de luz y por lo tanto no se realizará la instrucción indicada. En contraste, Bluetooth puede funcionar aun estando un dispositivo en un lugar cerrado siempre y cuando no sobrepase la distancia estipulada por la tecnología.

2.2 FUNCIONAMIENTO DE REDES INALÁMBRICAS

Las redes inalámbricas es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de esta. Se comunican a través de medios de transmisión no guiados, siendo el medio por aire el que se utiliza en tecnología inalámbrica. Se radian señales de radio frecuencia por medio de una antena y luego se recibe esta energía con otra antena.

Está tecnología tiene como prioridad el poder comunicar computadoras mediante tecnología inalámbrica. Dichas redes inalámbricas facilitan enormemente el trabajo en lugares donde la computadora no puede permanecer en un solo lugar, como por

ejemplo, en las oficinas que se encuentren en varios pisos.

Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en salas de reuniones, pasillos, restaurantes, etc. Además ofrecen una movilidad e instalación muy sencilla. Esto permite al usuario viajar a distintas ubicaciones y aun tener acceso a los datos de red.

Cabe mencionar una aclaración pertinente no se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, ya que éstas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra óptica logran velocidades aún mayores; se piensa que en un futuro las redes inalámbricas logren alcanzar velocidades de 10 Mbps.

Una opción también podría ser el mezclar las redes cableadas y las inalámbricas, y así generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Teniendo en consideración que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de redes inalámbricas:

1.- De Larga Distancia.- Se utilizan para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta

varios países vecinos (mejor conocido como Redes de Area Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

2.- De Corta Distancia.- Se utilizan principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información con un alto costo, debido a que los módems celulares actualmente son más caros y delicados que los tradicionales, ya que requieren de una circuitería especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no representa problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

- La carga de los teléfonos se termina rápidamente.
- La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
- Velocidades de transmisión bajas.

Todas estas desventajas propician que la comunicación celular se emplee poco, o únicamente para archivos muy pequeños como cartas,

planos, etc. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable para algunas situaciones.

Otra opción que existe en redes de larga distancia son las llamadas: Red Pública de Conmutación de Paquetes por Radio.

Estas redes no presentan problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes emplean la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringida por la propia organización de sus sistemas de cómputo.

2.2.1 TOPOLOGÍAS DE REDES LAN INALÁMBRICAS

Las redes LAN inalámbricas están construidas bajo dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc".

La topología de infraestructura (ver figura 2.1) es aquella que extiende una red LAN con cable existente para de ahí incorporar dispositivos inalámbricos mediante una estación base, llamada punto de acceso. Este punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. También el punto de acceso coordina la transmisión y

recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En el modo de infraestructura, se pueden tener varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

En la topología ad hoc, (ver figura 2.2) los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. A diferencia de la estructura en ésta cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central.

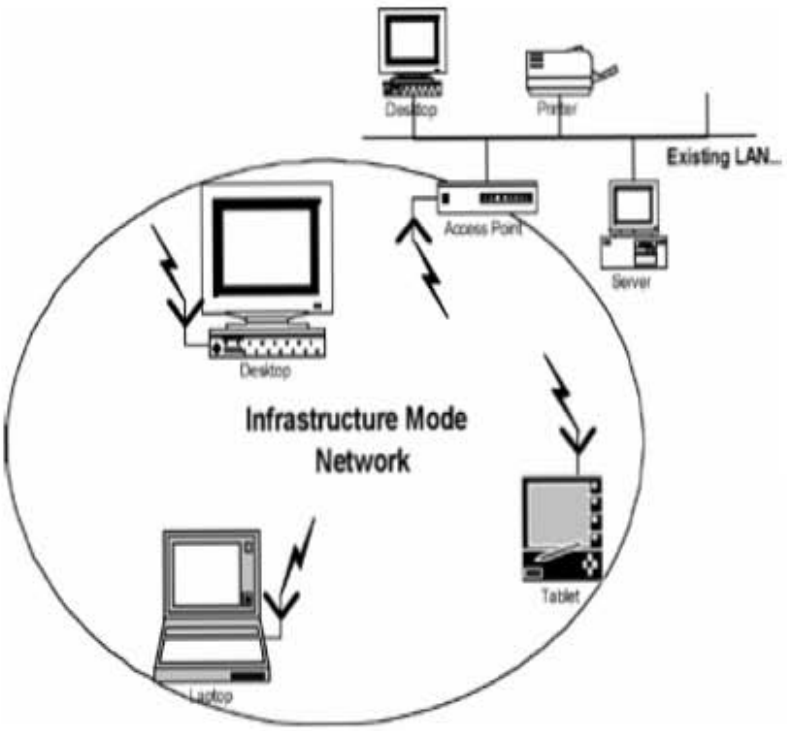

Figura2.1 Red de la modalidad de infraestructura Fuente: www.google.com

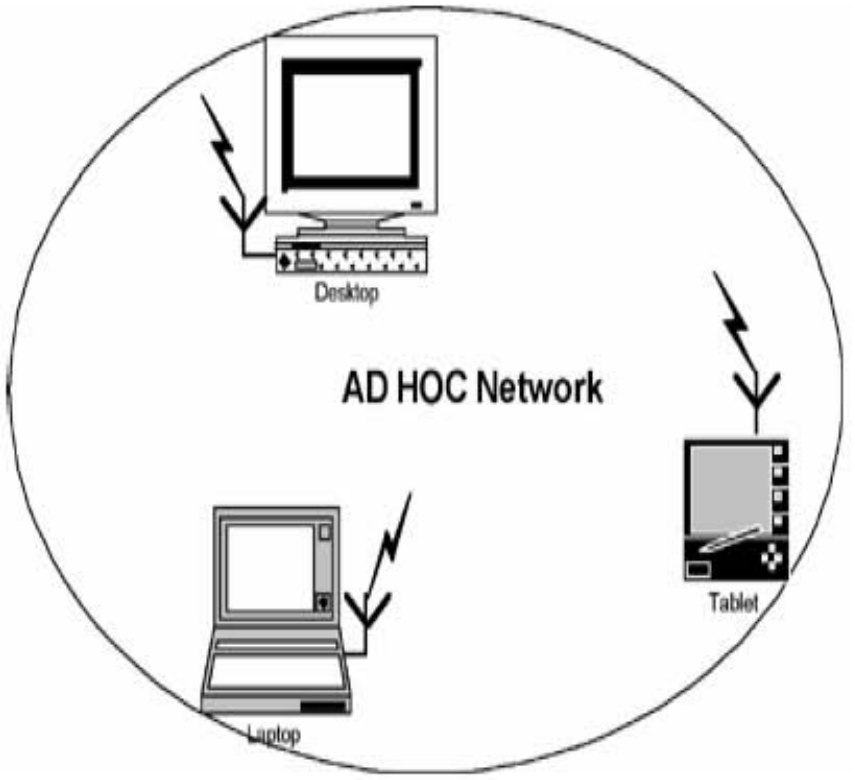

Figura 2.2 Red ad hoc Fuente: www.google.com

Estas redes inalámbricas ad hoc permiten a los usuarios móviles colaborar, transferir archivos o comunicarse de algún otro modo mediante su PC o dispositivos inteligentes sin cables.

2.2.2 DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA MODALIDAD DE INFRAESTRUCTURA

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los

puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

Luego la estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación básicamente permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En el proceso de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones.

Cabe mencionar que en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

2.2.3 DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA MODALIDAD AD HOC

En esta red sólo hay dispositivos inalámbricos presentes.

Muchas de las operaciones que controla el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no tiene todavía algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto también pasa en el caso de las redes LAN inalámbricas. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas.

Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala, de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad sin interrupciones en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) y métrica que se agrega a los parámetros de configuración.

2.2.3 RETOS PARA LOS USUARIOS MÓVILES

Cuando un usuario o una estación se desplaza de un punto de acceso a otro punto de acceso, se debe mantener una asociación entre la tarjeta NIC y un punto de acceso para poder mantener la conectividad de la red. Esto puede plantear un problema especialmente complicado si la red es grande y el usuario debe cruzar límites de subredes o dominios de control administrativo.

Si el usuario cruza un límite de subred, la dirección IP asignada originalmente a la estación puede dejar de ser adecuada para la nueva subred. Si la transición supone cruzar dominios administrativos, es posible que la estación ya no tenga permiso de acceso a la red en el nuevo dominio basándose en sus credenciales.

Más allá del simple desplazamiento dentro de un campus corporativo, otros escenarios de usuarios móviles son muy reales. Los aeropuertos y restaurantes agregan conectividad inalámbrica con Internet y las redes inalámbricas se convierten en soluciones de red populares para el hogar.

Ahora es más probable que el usuario pueda abandonar la oficina para reunirse con alguien de otra compañía que también disponga de una red inalámbrica compatible. De camino a esta reunión, el usuario necesita recuperar archivos desde la oficina principal y podría encontrarse en una estación de tren, un restaurante o un aeropuerto con acceso inalámbrico.

Para este usuario sería de mucha utilidad poder autenticarse y utilizar esta conexión para obtener acceso a la red de la empresa. Cuando el usuario llegue a su destino, puede que no tenga permiso de acceso a la red local de la empresa que va a visitar. Sin embargo, sería inmejorable que el usuario pudiera obtener acceso a Internet en este entorno extraño. Entonces, dicho acceso podría utilizarse para crear una conexión de red privada virtual con la red de su empresa. Después, el usuario podría irse a casa y desear conectarse a la red doméstica para descargar o imprimir archivos para trabajar esa tarde. Ahora, el usuario se ha desplazado a una nueva red inalámbrica, que posiblemente incluso puede ser de la modalidad ad hoc.

Para este ejemplo, la movilidad es una situación que debe pensarse muy detenidamente. La configuración puede ser un problema para el usuario móvil, ya que las distintas configuraciones de red pueden suponer un reto si la estación inalámbrica del usuario no tiene capacidad para configurarse automáticamente.

2.2.5 RETOS DE CONFIGURACIÓN

Cuando se tiene una conexión de red inalámbrica y la complejidad ha aumentado, posiblemente hay muchas más configuraciones que realizar. Por ejemplo, podría ser necesario configurar el SSID de la red a la que se va a realizar la conexión. O bien, podría ser necesario configurar un conjunto de claves WEP de seguridad; posiblemente, varios conjuntos de claves si es necesario conectarse a varias redes. Podría ser necesario tener una configuración para el trabajo, donde la red funciona en modo de infraestructura, y otra configuración para el

domicilio, donde funciona en modo ad hoc. Entonces, sería necesario elegir qué configuración se va a utilizar en función del lugar donde nos encontremos.

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto es cierto también en el caso de las redes LAN inalámbricas. Algunos retos saltan a la vista de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas. Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala, de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad sin interrupciones en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) y métrica que se agrega a los parámetros de configuración.

2.2.6 CARACTERÍSTICAS DE FUNCIONAMIENTO DE LAS LAN INALÁMBRICAS QUE UTILIZAN SALTOS DE FRECUENCIA

Tabla 2.2 Características de las lan inalámbricas

Característica	**Funcionamiento**
Tipo de conexión	Expansión de espectro (secuencia directa o saltos de frecuencia)
Espectro	Banda ISM de 2.4 GHZ(banda de aplicaciones industriales, científicas y médicas).
Potencia de transmisión	100 milivatios (mW)
Velocidad de transferencia de datos	1 Mbps 0o 2 Mbps utilizando saltos de frecuencia; 11 Mbps utilizando secuencia directa.
Alcance	Hasta 100 metros entre el punto de acceso los clientes.
Tipos de estaciones	Múltiples dispositivos por punto de acceso; múltiples puntos de acceso por red.
Canales de Voz	Voz sobre IP

Seguridad de los datos	Autenticación: desafío-respuesta entre punto de acceso y cliente mediante WEP (Wired Equivalent Privacy, confidencialidad equivalente a cable). Cifrado: estándar de 40; opcional de 128 bits.
Direccionamiento	Cada dispositivo tiene una dirección MAC (dirección de acceso al medio físico) de 48 bits que se utiliza para establecer una conexión con otro dispositivo.

2.3 FUNCIONAMIENTO DE BLUETOOTH

La tecnología inalámbrica bluetooth se basa en transceptores de corto alcance diminutos y de bajo costo en los dispositivos móviles disponibles hoy en día, ya sea que vengan integrados directamente en tarjetas de expansión existentes o que sean añadidos mediante dispositivos adaptadores, como una tarjeta pc-card insertada en un equipo portátil.

Cada dispositivo deberá estar equipado con un microchip que transmite y recibe en la frecuencia de 2.4 Ghz (disponible en todo el mundo), teniendo un radio de acción de los 10 metros, hasta los 100 metros y con velocidad de transferencia de hasta 721kbps.

2.3.1 ESPECIFICACIONES DE LA TECNOLOGÍA

La especificación de Bluetooth define un canal de comunicación de máximo 720Kb/seg con rango óptimo de 10m (opcionalmente 100m). Para utilizar Bluetooth hay que equipar cada dispositivo con un microchip (figura 2.3) que transmite y recibe, hasta 1 Mbit/s, en la frecuencia de 2,4 GHz, en una banda ISM (Industrial Scientific Medical), mundialmente disponible y que no requiere de licencia, con algunas variaciones de ancho de banda en países como España, Francia y Japón.

Figura 2.3 Microchip Bluetooth Fuente: http://www.umtsforum.net

Dicha frecuencia con la que trabaja está en el rango de 2.4 a 2.48Ghz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en full duplex[3] con un máximo de 1600 saltos/seg. Los saltos de frecuencia se dan entre un total de 79 frecuencias con

[3] Con una operación full-duplex, las transmisiones pueden ocurrir en ambas direcciones al mismo tiempo. También se le conoce como líneas simultánea de doble sentido.

intervalos de 1Mhz; esto permite brindar seguridad y robustez. La potencia de salida para transmitir a una distancia máxima de 10m es de 0dBM (1 mW), mientras que la versión de largo alcance transmite entre -30 y 20dBM (100 mW).

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideo una solución que se puede implementar en un solo chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.

El protocolo de banda base (canales simples por línea) combina switching de circuitos y paquetes. Para asegurar que los paquetes no lleguen fuera de orden, los slots[4] pueden ser reservados por paquetes síncronos, un salto diferente de señal es usado para cada paquete. Por otro lado, el switching de circuitos puede ser asíncrono o síncrono. Tres canales de datos síncronos (voz), o un canal de datos síncrono y uno asíncrono, pueden ser soportados en un solo canal. Cada canal de voz puede soportar una tasa de transferencia de 64 Kb/s en cada sentido, la cual es suficientemente adecuada para la transmisión de voz. Un canal asíncrono puede transmitir como mucho 721 Kb/s en una dirección y 56 Kb/s en la dirección opuesta; sin embargo, para una conexión asíncrona es posible soportar 432,6 Kb/s en ambas direcciones si el enlace es simétrico.

El sistema se basa en un chipset llamado con el mismo nombre, bluetooth, que se encarga de establecer conexión mediante señales

[4] En comunicaciones es una banda de frecuencia estrecha.

de radio con dispositivos que poseen esta misma tecnología. Tras detectar el otro dispositivo comienza la comunicación.

El máximo número de dispositivos que se pueden conectar al mismo tiempo son de 8, a esta red se le denomina ***picorred***[5]. Posee un máximo de ancho de banda de 1 Mbit/seg.

Además ha sido diseñado para trabajar en un entorno multiusuario.

Así podemos construir una red en un área de 10 cm. de mínimo a 10 metros como máximo pudiendo llegar a incrementarse esta distancia aumentando la señal emitida. En cuanto a su velocidad puede llegar a 721 Kbps y poseer tres canales de voz.

Diez picorredes pueden coexistir en un mismo lugar de cobertura de radio. La seguridad se preserva gracias a que cada enlace se decodifica y protege contra interferencias de intrusos.

2.3.2 ESTRUCTURA DE UNA PICORRED

Una picorred está formada como máximo por un dispositivo que se denomina *Master* y como mínimo por otro dispositivo llamado *Esclavo*.

El Master se encarga de sincronizar la comunicación entre los diferentes dispositivos esclavos.

A cada picorred independiente se le denomina Scatternet[6](figura 2.4).

[5] Picorred.- Colección de dispositivos (de 2 a 8) conectados por medio de la tecnología.
[6] Scatternet: varias picorred independientes y no sincronizadas forman una scatternet

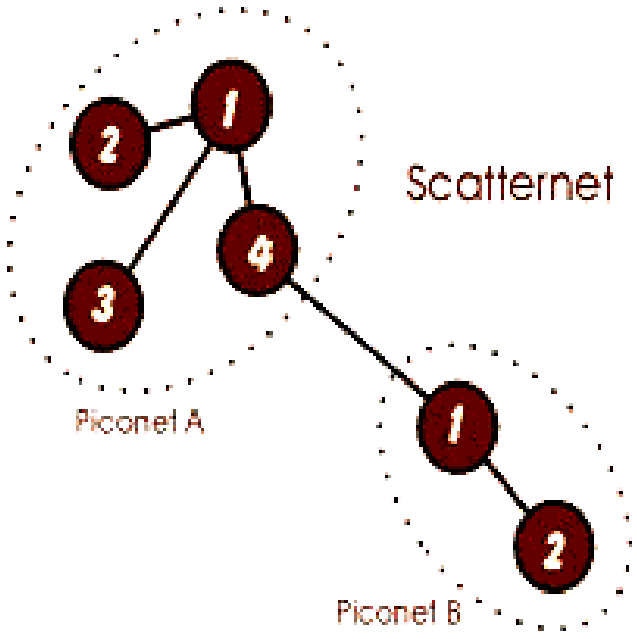

Figura 2.4. Red Scatternet Fuente: http://www.datex-ohmeda.es

Las topologías de las redes Bluetooth puede ser punto-a-punto o punto-a-multipunto.

Los dispositivos, se comunican en redes denominadas piconets. Estas redes tienen posibilidad de crecer hasta tener 8 conexiones punto a punto. Además, se puede extender la red mediante la formación de scatternets. Una scatternet es la red producida cuando dos dispositivos pertenecientes a dos piconets diferentes, se conectan.

En una piconet, un dispositivo debe actuar como master, enviando la información del reloj (para sincronizarse) y la información de los saltos de frecuencia. El resto de los dispositivos actúan como slaves.

2.4 ARQUITECTURA BLUETOOTH

En lo referente a la arquitectura del hardware, un dispositivo Bluetooth está compuesto por dos partes: un dispositivo de radio, encargado de modular y transmitir la señal, y un controlador digital, integrado por una CPU, encargada de atender las instrucciones relacionadas con Bluetooth del dispositivo anfitrión, y un procesador de señales digitales, sobre el que corre un software denominado Link Controller, encargado del cumplimiento de los protocolos de comunicación entre los dispositivos con esta tecnología, además de que el enlace sea en todo momento seguro y estable.

2.4.1 ARQUITECTURA DE HARDWARE

El hardware que compone el dispositivo Bluetooth está compuesto por dos partes. Un dispositivo de radio, encargado de modular y transmitir la señal, y un controlador digital. El controlador digital (figura 2.5) está compuesto por un CPU, por un procesador de señales digitales (DSP - Digital Signal Processor) llamado Link Controller (o controlador de Enlace) y de los interfaces con el dispositivo anfitrión.

El LC o Link Controller está encargado de hacer el procesamiento de la banda base y del manejo de los protocolos ARQ y FEC de capa física. Además, se encarga de las funciones de transferencia (tanto asíncrona como síncrona), codificación de audio y encripción de datos.

El CPU del dispositivo se encarga de atender las instrucciones relacionadas con Bluetooth del dispositivo anfitrión, para así simplificar su operación. Para ello, sobre el CPU corre un software denominado Link Manager que tiene la función de comunicarse con otros dispositivos por medio del protocolo LMP.

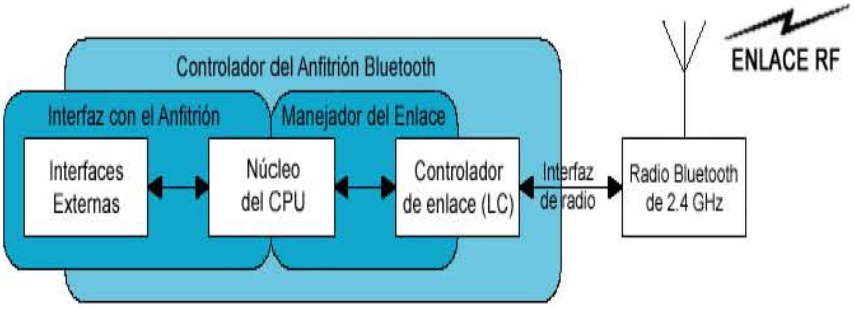

Figura 2.5 Controlador digital Fuente: www.bluetooth.ericsson.se

Entre las tareas realizadas por el LC y el Link Manager, destacan las siguientes:

- Envío y recepción de datos.
- Empaginamiento y peticiones.
- Determinación de conexiones.
- Negociación y determinación de tipos de enlace, por ejemplo SCO o ACL.
- Determinación del tipo de cuerpo de cada paquete.

- Ubicación del dispositivo en modo sniff o hold.

2.4.2 ARQUITECTURA DE SOFTWARE

Buscando ampliar la compatibilidad de los dispositivos Bluetooth, los dispositivos que se apegan al estándar utilizan como interfaz entre el dispositivo anfitrión (laptop, teléfono celular, etc) y el dispositivo Bluetooth como tal (chip Bluetooth) una interfaz denominada HCI (Host Controller Interface).

Los protocolos de alto nivel como el SDP (protocolo utilizado para encontrar otros dispositivos Bluetooth dentro del rango de comunicación, encargado, también, de detectar la función de los dispositivos en rango), RFCOMM (protocolo utilizado para emular conexiones de puerto serial) y TCS (protocolo de control de telefonía) interactúan con el controlador de banda base a través del protocolo L2CAP (Logical Link Control and Adaptation Protocol). El protocolo L2CAP se encarga de la segmentación y reensamblaje de los paquetes para poder enviar paquetes de mayor tamaño a través de la conexión Bluetooth.

2.5 PROTOCOLOS

Los protocolos son reglas o especificaciones que indican la manera en la que los dispositivos intercambian información. Para cada tipo de tecnología de red, incluyendo la de la especificación Bluetooth, hay un conjunto de protocolos o reglas que definen exactamente cómo se

pasan los mensajes por el enlace. El protocolo define el formato de esos mensajes, incluyendo qué partes se reservan para cosas como la dirección, el control de errores y los datos de usuario.

Los protocolos que definen cómo se pasa el tráfico de señales por el enlace se parecen mucho a los protocolos que todos observamos en la vida diaria. Cuando conducimos un coche hacia un cruce, por ejemplo, sabemos lo que hemos de hacer porque observamos el protocolo que indica el semáforo: verde para pasar, amarillo para prevenir y rojo para parar. En los raros casos donde no encontremos semáforos ni señales, hay cierta confusión entre los conductores sobre qué vehículo ha de pasar. Cuando esto sucede el tráfico puede ser muy lento, especialmente si hay colisiones. Si uno circula por esta carretera corre el riesgo de llegar a su destino demasiado tarde.

Si no hubiera protocolos comúnmente aceptados, una red no podría funcionar correctamente, ya que los fabricantes del hardware y los desarrolladores de software harían las cosas a su manera. Y el resultado serían productos propios que no podrían comunicarse entre sí en la misma red.

2.5.1 INTERCONEXIÓN DE SISTEMAS ABIERTOS

La organización internacional de estandarización ISO (International Standards Organization) dictó el modelo de referencia OSI en 1974. Su objetivo del modelo de 7 niveles era separar las diversas funciones de red para fomentar la interoperabilidad entre los productos de diferentes fabricantes. Cada nivel aporta ciertas funciones de

protocolo que en combinación aseguran un intercambio transparente de información libre de errores entre varios dispositivos interconectados.

2.5.2 MODELO DE REFERENCIA OSI DE SIETE NIVELES

Tabla 2.3 Niveles del modelo OSI

Nivel OSI	Descripción	Funciones incluidas
Aplicación	Define la forma en la que las aplicaciones interactúan con la red.	Correo electrónico, transferencia de archivos.
Presentación	Define la forma en la que los datos se formatean, se presentan, se convierten y se codifican.	Traducción de códigos de caracteres, conversión de dato, compresión de datos, cifrado de datos.
Sesión	Define el procedimiento para establecer, mantener y desconectar un enlace de comunicaciones entre dispositivos de una red.	Sincronización de datos, búsqueda de nombres, autenticación y registro.
Transporte	Define los procedimientos para garantizar una transmisión de datos confiable.	Traducción de la dirección física/lógica, calidad de servicio, elección de ruta.

Red	Define los procedimientos para encaminar datos a través de sistemas intermedios hasta el nodo de destino correcto.	Traducción de la dirección física/lógica, calidad de servicio, elección de ruta.
Enlace de datos	Valida la integridad del flujo de datos entre un nodo y otro sincronizando los bloques de datos y controlando el flujo de datos.	Ensamblado/desensambla - do de tramas, comproba - ción de errores de tramas, retransmisión de tramas.
Físico	Define las características físicas y eléctricas del medio a través del cual se transmi- ten los datos en forma de unos y ceros.	Cableado (incluyendo la definición de los termina- les para los conectores de los cables), interfaces de red, señalización de transmisión/recepción, detección de errores de señalización en el medio físico.

2.5.3 BANDA BASE

El nivel de banda base permite el enlace físico de RF entre unidades Bluetooth dentro de una picorred. Como los sitemas RF Bluetooth

utilizan la tecnología de expansión de espectros por saltos de frecuencia, donde los paquetes se transmiten en franjas de tiempo predefinidas por frecuencias predefinidas; este nivel utiliza procedimientos de averiguación y localización para sincronizar la frecuencia de saltos de transmisión y los relojes de los diferentes dispositivos Bluetooth.

Este nivel proporciona los dos diferentes enlaces físicos, con sus correspondientes paquetes de banda base: síncrono orientado a la conexión (SCO, Synchronous Connection-Oriented) y asíncrono sin conexión (ACL, Asynchronous Connectionless), que se pueden transmitir de forma multiplexada sobre el mismo enlace RF. Los paquetes ACL sólo se utilizan para datos, mientras que un paquete SCO puede contener sólo audio o una combinación de audio y datos. Todos los paquetes de audio y de datos pueden ofrecerse con diferentes niveles de corrección de errores, y se pueden cifrar para asegurar la confidencialidad. Además, a los mensajes de control y de gestión de enlace se les asigna un canal especial a cada uno.

Los paquetes que contienen datos de audio se pueden transferir entre uno o más dispositivos Bluetooth, haciendo posible la existencia de varios modelos de uso. Los datos de audio en los paquetes SCO se encaminan directamente hacia y desde la banda base, y no pasan por L2CAP. El modelo de audio es relativamente sencillo dentro de la

especificación Bluetooth; dos dispositivos Bluetooth cualesquiera pueden enviar y recibir datos de audio entre ellos simplemente abriendo un enlace audio.

2.5.4 PROTOCOLO DE GESTOR DE ENLACE (LMP)

LMP es el responsable de la configuración y control del enlace entre dispositivos Bluetooth, incluyendo el control y negociación del tamaño de los paquetes de banda base. También se utiliza para la seguridad: autentificación y cifrado; generación, intercambio y comprobación de las claves de cifrado de enlace. LMP también controla los modos de administración de energía y los ciclos de trabajo del dispositivo de radio Bluetooth, y los estados de conexión de una unidad Bluetooth dentro de una picorred.

El gestor de enlace del lado receptor filtra e interpreta los mensajes LMP, por lo que nunca pasan los niveles superiores. Los mensajes LMP tienen una prioridad más elevada que los datos de usuario. Si un gestor de enlace necesita enviar un mensaje, no se verá retrasado por el tráfico L2CAP. Además, los mensajes LMP no se confirman explícitamente, ya que el canal lógico ofrece un enlace suficientemente fiable, lo que hace a las confirmaciones innecesarias.

2.5.5 PROTOCOLO DE ADAPTACIÓN Y CONTROL DE ENLACE LÓGICO (L2CAP)

El protocolo de adaptación y control del enlace lógico (L2CAP) soporta multiplexación de protocolos de nivel superior, la segmentación y reensamblado de paquetes, y los mecanismos de calidad de servicio (QoS, Quality of Service). L2CAP permite que protocolos y aplicaciones de nivel superior transmitan y reciban paquetes de datos

de hasta 64 kilobytes de longitud. Aunque el protocolo de banda base ofrece los tipos de enlace SCO y ACL, L2CAP está definido sólo para enlaces ACL y no hay planeado soporte para enlaces SCO. Los canales con calidad de voz para aplicaciones de audio y telefonía suelen funcionar sobre enlaces SCO de banda base. Sin embargo, los datos de audio pueden ensamblarse en paquetes y enviarse utilizando protocolos de comunicación que funcionen sobre L2CAP.

2.5.6 PROTOCOLO DE DESCUBRIMIENTO DE SERVICIOS (SDP)

Los servicios de descubrimiento son un elemento importante en la arquitectura Bluetooth, ya que proporcionan la base para todos los modelos de uso. Por medio de SDP, se puede consultar la información de los dispositivos, los servicios que ofrecen y las características de dichos servicios. Habiendo localizado los servicios disponibles en las cercanías, el usuario puede elegir cualquiera de ellos. Después de eso, se puede establecer una conexión entre dos o más dispositivos Bluetooth.

2.6 PROTOCOLOS DE SUSTITUCIÓN

2.6.1 RFCOMM

RFCOMM es un protocolo de emulación de línea serie basado en un subconjunto de estándar TS 07.10 del Instituto Europeo de Estándares de Telecomunicaciones (ETSI, European Telecomunications Standards Institute), que también se utilizan para

los dispositivos de comunicaciones GSM (Global System for Mobile, sistema global para móviles). El ETSI es una organización sin ánimo de lucro que elabora los estándares de telecomunicaciones que se utilizan en Europa.

2.6.2 CARACTERÍSTICAS DEL RFCOMM

- Emula las señales de control y datos RS-232 sobre la banda base, proporcionando ambas capacidades de transporte a los servicios de niveles superiores que utilizan el cable serie como mecanismo de transporte.
- Soporta aplicaciones que hacen uso del puerto serie de un dispositivo.
- Sólo se ocupa de la conexión entre dispositivos Bluetooth en el caso de una conexión directa, o entre el dispositivo Bluetooth y un módem en el caso de una red.
- Puede soportar otras configuraciones, como módulos que se comunican vía tecnología inalámbrica Bluetooth, además de ofrecer una interfaz de cable por otro.
- No es realmente un módem pero ofrece un servicio similar.

2.6.3 PROTOCOLOS DE CONTROL DE TELEFONÍA

TCS Binary o TCS BIN es un protocolo orientado a bit que define la señalización de control de llamada para establecer llamadas de voz y datos entre dispositivos Bluetooth.

2.6.4 CARACTERÍSTICAS

- Define los procedimientos de gestión de movilidad para manejar grupos de dispositivos TCS Bluetooth.
- TCS BIN se basa en la recomendación Q.931 emitida por la Unión Internacional de Telecomunicaciones (ITU-T), agencia de las Naciones Unidas que coordina los estándares para redes y servicios de telecomunicación global.
- Q.931 es la especificación ITU-T para el control básico de llamadas bajo RDSI (Red Digital de Servicios Integrados).
- TCS BIN junto con el SIG Bluetooth definieron un conjunto de comandos AT los cuales indican cómo puede controlarse un módem y un teléfono móvil en varios modelos de uso.

2.6.5 PROTOCOLOS ADOPTADOS

Estos protocolos denominados antiguos se reutilizan en la tecnología Bluetooth, para ayudar y asegurar un correcto funcionamiento de estas aplicaciones con aplicaciones más modernas diseñadas específicamente para dispositivos Bluetooth.

2.6.5.1 PPP

- Desarrollado por el IETF (Internet Engineering Task Force, Grupo Especial de Ingeniería Internet).

- Este protocolo define la manera de cómo se transmiten los datagramas[7] IP sobre enlaces serie punto a punto.

2.6.5.1.1 COMPONENTES PRINCIPALES DEL PPP

A) ENCAPSULACIÓN

Proporciona un método de encapsular los datagramas sobre enlaces serie. Ofrece un protocolo de encapsulación sobre enlaces síncronos orientados a bit y enlaces asíncronos con ocho bits de datos y sin paridad. La encapsulación también ofrece el multiplexado simultáneo de diferentes protocolos de nivel de red sobre el mismo enlace. Proporciona una solución común para una fácil conexión entre una amplia variedad de máquinas host, puentes y encaminadores.

B) PROTOCOLO DE CONTROL DE ENLACE (LCP, LINK CONTROL PROTOCOL)

PPP ofrece un protocolo de control de enlace para asegurar su portabilidad a una amplia variedad de entornos. LCP se utiliza para alcanzar un acuerdo automático de las opciones de formato de encapsulación, para gestionar la variación en los límites de los tamaños de los paquetes, para autentificar la identidad de la otra parte del enlace y así determinar cuándo un enlace funciona correctamente y cuándo ya no existe.

[7] Datagramas.- Son unidades de datos que se transportan sobre el enlace por medio de un mecanismo optimizado, pero sin garantía de entrega.

C) PROTOCOLOS DE CONTROL DE RED

Los enlaces punto a punto tienden a tener muchos problemas relacionados con los protocolos de red. Por ejemplo, la asignación y gestión de las direcciones IP, un problema incluso en entornos LAN, es difícil sobre enlaces punto a punto.

Este tipo de problemas es resuelto por protocolos de control de red, los cuales gestionan las necesidades específicas de sus respectivos protocolos de nivel de red.

2.6.5.2 TCP/UDP/IP

Estos protocolos se emplean para comunicaciones a través de internet. Se incluyen en numerosos dispositivos, entre ellos todos los modelos de computadoras de escritorio y portátiles, así como minicomputadoras, grandes sistemas y supercomputadoras.

2.6.5.3 PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

- Protocolo confiable extremo a extremo, orientado a la conexión.

- Soporta aplicaciones multired.

- Envía los datos que se le entregan en forma de datagramas IP o paquetes al proceso apropiado en el host receptor.

- Define los procedimientos para fragmentar los datos en paquetes, recomponerlos para reconstruir los datos originales en el extremo receptor y emitir peticiones de retransmisión para sustituir los paquetes perdidos o dañados.

- Todos los paquetes se almacenan temporalmente hasta que llegan los últimos, para poder ponerlos en el orden correcto.

- Si un paquete llega dañado, se elimina y se reenvía otro en respuesta a una petición de retransmisión.

2.6.5.4 PROTOCOLO DE DATAGRAMAS DE USUARIO (UDP)

- Pasa mensajes individuales a IP para su transmisión con un mecanismo optimizado, no tiene garantía de entrega.

- Resulta útil para consultas rápidas a bases de datos.

- También es de utilidad en el envío de mensajería simple entre aplicaciones.

2.6.5.5 PROTOCOLO INTERNET (IP)

- Transporta datagramas entre diferentes redes a través de encaminadores que procesan paquetes desde un sistema autónomo (AS, Autonomous System) a otro.

- Cada dispositivo AS tiene una dirección IP exclusiva. El protocolo IP añade su propia cabecera y una suma de comprobación, para asegurarse de que los datos son encaminados correctamente. Este proceso es ayudado por la presencia de mensajes de actualización de encaminamiento, que mantienen las tablas de direcciones actualizadas en cada encaminador.

- Se emplean varios tipos de mensajes de actualización, dependiendo del conjunto de subredes incluidas en un dominio de gestión.

- Las tablas de encaminamiento enumeran los diversos nodos de las subredes, así como los caminos entre los nodos. Si un paquete de datos es demasiado grande, el nivel superior TCP lo segmenta en paquetes más pequelos.

- Implementando este estándar en Bluetooth, permite la comunicación con cualquier otro dispositivo conectado a Internet, es decir, se emplea como un puente hacia internet.

2.6.5.6 PROTOCOLO OBEX

Es un protocolo de nivel de sesión desarrollado originalmente con el nombre de IrOBEX por la Asociación de datos por infrarrojos.

- Su objetivo es soportar el intercambio de objetos de forma simple y espontánea.

- Se basa en el modelo cliente-servidor y es independiente del mecanismo de transporte.

- En mayo de 1999, OBEX se convirtió en el primer protocolo común para las dos especificaciones inalámbricas: Bluetooth e Infrarroja.

- Nokia fue la primera compañía celular en comenzar a emplear este protocolo para el intercambio de objetos.

2.6.5.7 PROTOCOLO DE APLICACIONES INALÁMBRICAS (WAP)

WAP es una especificación para enviar y leer mensajes y contenido Internet en pequeños dispositivos inalámbricos.

La fortaleza de WAP reside en que abarca múltiples estándares de enlace por aire y, dentro de la tradición Internet, permite a los

publicadores de contenido y desarrolladores de aplicaciones despreocuparse del mecanismo de distribución específico.

Emplea la transmisión binaria para una mayor compresión de los datos, y está optimizado para largos retardos y un ancho de banda bajo-medio. Las sesiones WAP resuelven el problema de cobertura intermitente y pueden funcionar sobre una amplia variedad de transportes inalámbricos, utilizando IP donde sea posible y otros protocolos optimizados donde IP no es posible.

Existe un par de cosas para las que WAP resulta bueno en el entorno Bluetooth: la distribución de información y el procesamiento transparente.

"La distribución de información, un cliente WAP que emplee la tecnología inalámbrica Bluetooth descubrirá la presencia de un servidor WAP utilizando el protocolo de descubrimiento de servicios (SDP). Al momento de detectar un servicio, se determina la dirección del servidor WAP; cuando el cliente obtiene la dirección establece una conexión con el servidor y puede acceder a la información o al servicio ofrecido por ese servidor según un esquema de suscripción o de extracción. El cifrado y autenticación para seguridad entre cliente y servidor vienen dados por el protocolo de seguridad de nivel de transporte inalámbrico (WTLS), que es importante para salvaguardar la confidencialidad del comercio electrónico y las aplicaciones de procesamiento transparente.[8]"

[8] J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed**.** Mc Graw Hill, 2002, pág 103.

El procesamiento transparente es la capacidad de entrar a una computadora y controlar su funcionamiento desde un dispositivo móvil.

Como hemos visto, los protocolos Bluetooth están dirigidos a facilitar el rápido desarrollo de aplicaciones que puedan aprovecharse de la tecnología inalámbrica Bluetooth.

Además, otros protocolos como el RFCOMM, se ha adoptado partiendo de protocolos existentes, y sólo se ha modificado ligeramente para los propósitos de la especificación Bluetooth.

Los protocolos de nivel superior como WAP, se emplean sin modificaciones, como también así, las aplicaciones existentes se pueden reutilizar para trabajar con la tecnología inalámbrica Bluetooth sin poner en riesgo la interacción entre las aplicaciones Bluetooth y los dispositivos de diferentes fabricantes.

El propósito de la especificación Bluetooth es promover el desarrollo de aplicaciones ínter operables destinadas a los modelos de uso de mayor prioridad. Sin embargo, la especificación Bluetooth también sirve como plataforma para desarrollos posteriores, alentando así a los fabricantes del hardware y software para que creen más modelos de uso dentro de esa plataforma. La tecnología inalámbrica Bluetooth, combinada con las diferentes capacidades de las computadoras y dispositivos de comunicación existentes en la actualidad hace que las posibilidades en cuanto a futuras aplicaciones inalámbricas sean virtualmente sin límites.

CAPÍTULO III. BLUETOOTH Y LAS COMUNICACIONES INALÁMBRICAS DE TERCERA GENERACIÓN

Como nos hemos dado cuenta Bluetooth esta ligado a la telefonía celular desde sus inicios y hasta el día de hoy, podemos apreciar en nuestras vidas diarias como implementamos está tecnología en los celulares de tercera generación; como por ejemplo al enviar un video, una canción o una foto.

Así pues el área de la telefonía a logrado grandes avances en lo que a Internet se refiere, con los nuevos teléfonos celulares y el servicio móvil de Internet que ofrecen las compañías celulares podremos hacer muchas de las tareas que hacíamos desde nuestras computadoras, como leer correos electrónicos, consultar nuestro saldo bancario, transacciones e inclusive comprar algún producto desde nuestro teléfono. Y eso no es todo, con la tercera generación de telefonía móvil, tenemos la posibilidad de recibir y transferir grandes cantidades de información en el rango de Mbps, por lo que podremos recibir video o música en tiempo real desde nuestros teléfonos y otros dispositivos inalámbricos.

Es por esta afinidad que existe entre bluetooth y la telefonía celular que he introducido este capítulo y para conocerlo más a fondo comenzare por hablar de la historia que ha tenido a través del tiempo; hasta llegar a nuestros dias con la generación GSM, la cual

ha marcado una verdadera revolución tecnológica en cuanto a telefonía celular se refiere.

3.1 HISTORIA DE LA TELEFONÍA CELULAR.

AT&T introdujo el primer servicio telefónico móvil en los Estados Unidos el 17 de junio de 1946 en San Luis, Missouri. El sistema operaba con 6 canales en la banda de 150 MHz con un espacio entre canales de 60 KHz y una antena muy potente. Este sistema se utilizó para interconectar usuarios móviles (usualmente autos) con la red telefónica pública, permitiendo así, llamadas entre estaciones fijas y usuarios móviles. Un año después, el servicio telefónico móvil se ofreció en más de 25 ciudades de los EE.UU. y unos 44,000 usuarios en total aunque por desgracia había 22,000 más en una lista de espera de cinco años. Estos sistemas telefónicos móviles se basaban en una transmisión de Frecuencia Modulada (FM). La mayoría de estos sistemas utilizaban un solo transmisor muy poderoso para proveer cobertura a más de 80 km desde la base. Los canales telefónicos móviles de FM evolucionaron a 120 KHz del espectro para transmitir la voz con un ancho de banda de 3KHz. Aunque se esperaban mejoras en la estabilidad del transmisor, en la figura de ruido y en el ancho de banda del receptor.

La demanda para el servicio de telefonía móvil creció rápidamente y permaneció por detrás de la capacidad disponible en muchas de las ciudades de gran tamaño. Es increíble que a pesar de la demanda hayan pasado más de 30 años para cubrir las necesidades de telefonía móvil. La capacidad del sistema era menor que el tráfico que tenía que soportar, por ello, la calidad del servicio era terrible, las

probabilidades de bloqueo eran del 65% o más altas. La inutilidad del teléfono móvil disminuyó la frecuencia de su uso ya que los usuarios encontraron que era mejor prevenir no hablando en horas picos. Los usuarios y las compañías telefónicas se dieron cuenta que un conjunto de canales no sería suficiente para desarrollar un servicio telefónico móvil útil. Se necesitarían grandes bloques del espectro para satisfacer la demanda en áreas urbanas.

En 1949, la FCC dispuso más canales y la mitad se los dio a la compañía Bell System y la otra mitad a compañías independientes como la RCC(Radio Common Carriers), con la intención de crear la competencia y evitar los monopolios. Fue a mediados de los 50 cuando se creó el primer equipo para viajar en auto de menor tamaño. Esto sucedió en Estocolmo, en las oficinas centrales de Ericsson pero no fue sino 10 años después cuando los transistores redujeron en peso, tamaño y potencia para poder introducirlos al mercado.

En 1956, la Bell System comenzó a dar servicio en los 450 MHz, que era una nueva banda para tener una mayor capacidad. En 1958, la Richmond Radiotelephone Co. mejoró su sistema de marcado conectando rápidamente las llamadas de móvil a móvil. A mediados de los 60’s el Sistema Bell introdujo el Servicio Telefónico Móvil Mejorado (IMTS por sus siglas en inglés) con características mejoradas. Las mejoras en el diseño del transmisor y del receptor permitieron una reducción en el ancho de banda del canal de FM de 25-30 KHz.

A finales de los 60’s y principios de los 70’s el trabajo comenzó con los primeros sistemas de telefonía celular. Las frecuencias no eran reutilizadas en células adyacentes para evitar la interferencia en estos primeros sistemas celulares.

En enero 1969 la Bell System aplicó por primera vez el rehúso de frecuencias en un servicio comercial para teléfonos públicos de la línea del tren de N.Y. a Washington, D.C. Para desarrollar este sistema se utilizaron 6 canales en la banda de 450 MHz en nueve zonas a lo largo de una ruta de 380 km.

Se debe reconocer que la primera generación de radio celular analógico no fue una nueva tecnología pero si una nueva idea el de reorganizar la tecnología existente IMTS a gran escala. Mientras que las comunicaciones de voz utilizaron el mismo FM analógico que se había estado usando desde la II Guerra Mundial, dos mejoras importantes hicieron el concepto celular realidad. A principios de los 70’s se inventó el microprocesador; aunque los algoritmos complejos de control se implantaban en lógica con cables, el microprocesador hizo más fácil la vida de todos. La segunda mejora fue en el uso de un enlace de control digital entre el teléfono móvil y la estación base. No fue sino hasta marzo de 1977 cuando la FCC aprobó que Bell probara un sistema celular en Chicago.

En 1978, en EE.UU. comenzó a operar el Servicio Telefónico Móvil Avanzado o Advanced Mobile Phone Service AMPS. En ese año, 10 células cubrían 355000 km cuadradas en el área de Chicago, operando en las nuevas frecuencias en la banda de 800 MHz. Esta red utilizaba circuitos integrados LS, una computadora dedicada y un

sistema de conmutación, lo que probó que los sistemas celulares podían funcionar.

El desarrollo de AMPS fue muy rápido, un sistema comenzó a operar en mayo de 1978 en Arabia Saudita, otro en Tokio en diciembre de 1979 y el primero en nuestro país en 1981. Entonces, surgió por parte de la FCC otro requisito de competencia. Un proveedor de servicio celular tenía que coexistir con la Bell System en el mismo mercado (Bandas A y B). Entonces Ameritech entró en Chicago el 12 de octubre de 1983.

AT&T desarrolló un modelo junto con Motorola conocido como Dyna-TACS o TACS que significa Total Access Communications System, el cual se puso en marcha en Baltimore y en Washington D.C. por la compañía Cellular One el 16 de diciembre de 1983.

Otro estándar que surgió fue el de AURORA-400 en Canadá en febrero de 1983 utilizando equipo de GTE y NovAtel. Este sistema llamado descentralizado opera en los 420 MHz y utilizaba 86 células, funcionando mejor en áreas rurales por su poca capacidad pero cobertura amplia. En Europa, el sistema celular Telefonía Móvil Nórdico o Nordic Mobile Telephone System NMT450 inició operaciones en Dinamarca, Suecia, Finlandia y Noruega en el rango de 450 MHz. En 1985 la Gran Bretaña empezó a usar TACS en la banda de 900 MHz. Más tarde, Alemania Occidental implementó C-Netz, Los franceses Radiocom 2000, y los Italianos RTMI/RTMS. Todos ellos ayudaron a que hubiera nueve sistemas incompatibles, a diferencia de los EE.UU. que no sufrían de este problema. Desde aquí se pensó en un plan para crear un sistema digital único para Europa.

Para ejemplificar el desarrollo del mercado, la industria celular creció de menos de 204,000 suscriptores en 1985 a 1,600,000 en 1988 en EE.UU.

A finales de los 80's el interés emergió hacia los sistemas celulares de tipo digital, donde ambos, la voz y el control fueran digitales. El uso de tecnología digital para reproducción de discos compactos popularizó la calidad del audio digital. La idea de eliminar el ruido y proveer el habla clara hasta los límites de cada área de servicio fueron atractivos para los ingenieros y usuarios comunes.

En 1990, el sistema celular en EE.UU. agregó una nueva característica, el tráfico de la voz se convirtió en digital. Esto triplicó la capacidad con el muestreo, digitalización y multicanalización de las conversaciones. Para 1991, el servicio celular digital comenzó a emerger reduciendo el costo de las comunicaciones inalámbricas y mejorando la capacidad de manejar llamadas de los sistemas celulares analógicos.

En 1989 surge GSM primero conocido como Grupo Especial Móvil y luego como Sistema Global para Comunicaciones Móviles. Lo más destacado de él es que unifica los sistemas europeos. Desde 1993 los sistemas se estaban desbordando de usuarios en EE.UU., estos crecieron de medio millón en 1989 a más de trece millones en 1993. En 1994, Qualcomm, Inc. propuso un escenario de espectro esparcido para incrementar la capacidad. Construido en conocimientos anteriores, el Code Division Multiple Access CDMA o Acceso Múltiple por División de Código, sería en todos sus elementos digital, además de que prometía de 10 a 20 veces mayor capacidad. En estos días

más de la mitad de los teléfonos en el mundo operaban de acuerdo a los estándares de AMPS, y en su inicio más humilde nadie pensó que sería el que conviviría con TDMA o CDMA para obtener sistemas duales con tecnología analógica y digital.

El 14 de enero de 1997, la FCC abrió un nuevo grupo de frecuencias inalámbricas que permitiría el desarrollo de las tecnologías como CDMA: la banda de 1900. El PCS 1900 es la contraparte en frecuencia de GSM y aunque esta en desarrollo tiene un gran potencial.

En México, es hasta 1984 cuando Telcel obtiene la concesión para explotar la red de servicio radiotelefónico móvil en el área metropolitana de la Ciudad de México, bajo la denominación de "Radiomóvil Dipsa S.A. de C.V." operando en las bandas radiofónicas de 450-470 y 470-512 MHz. La Secretaría de Comunicaciones y Transportes convocó la introducción de la telefonía celular en nuestro país en las nueve diferentes regiones en que fue dividido. Aquí nace Iusacell, convirtiéndose en la primera compañía de telefonía celular en ofrecer el servicio en la Ciudad de México y en ese mismo año surge la marca Telcel ofreciendo los servicios de telefonía celular en la ciudad de Tijuana B.C. A partir de 1990 Telcel y Iusacell expanden los servicios de telefonía celular en el Distrito Federal y su zona metropolitana y paulatinamente ofrecen el servicio a escala nacional.

El día 31 de mayo de 1989 se presentó el "Plan Nacional de Desarrollo 1989-1994" donde menciona la importancia de las telecomunicaciones destacando los siguientes puntos :

- Múltiples empresas podrán desarrollar los servicios de transmisión conmutada de: datos, teleinformática, telefonía celular y otros.
- Las concesiones de telefonía celular se sujetarán a concurso de manera abierta, y así se garantizará la mejor oferta de servicios y contraprestación económica al Estado.

Y al igual que en el resto del mundo, el crecimiento de los teléfonos móviles ha sido muy grande, como por ejemplo Japón, que cuenta con 63.38 millones de celulares.

3.1.1 OBJETIVOS DE LA TELEFONÍA CELULAR

Cuando se definió el sistema de telefonía celular se plantearon objetivos que llevaron a la necesidad del concepto celular.
Estos objetivos son:
1) Alta capacidad de servicio*:* Capacidad para dar servicio de tráfico a varios miles de usuarios dentro de una
zona determinada y con un espectro asignado (Algunos cientos de canales de voz).
2) Uso eficiente del espectro: Uso eficiente de un recurso muy limitado como es el espectro de radio asignado al uso público.
3) Adaptabilidad a la densidad de tráfico*:* La densidad de tráfico varía en los distintos puntos de un área de servicio, el sistema se tiene que adaptar a estas variaciones.
4) Compatibilidad*:* Seguir un estándar, de forma tal de proveer el mismo servicio básico, con las mismas normas de operación a lo largo de todo el país.

5) Facilidad de extensión*:* Se trata que un usuario pueda cambiar de área de servicio pasando a una distinta y tener la posibilidad de comunicarse (Roaming).

6) Servicio a vehículos y portátiles.

7) Calidad de servicio: Implica seguir niveles estándares de bloqueo y calidad de voz.

8) Accesible al usuario*:* Es decir que el costo del servicio pueda ser afrontado por un gran número de personas.

3.2 GENERACIONES DE LA TELEFONÍA CELULAR

3.2.1 PRIMERA GENERACIÓN DE TELEFONÍA CELULAR

En 1971 se propuso el concepto de celular como un avanzado sistema de comunicación móvil. Esta intrigante idea proponía el reemplazo de las estaciones bases ubicadas en el centro de la ciudad por múltiples copias de tales estaciones de menor potencia distribuidas a lo largo del área de cobertura.

El concepto celular añade una dimensión espacial al modelo "trunking" usado anteriormente en la telefonía móvil. Estas células son ligadas a través de un centro de conmutación central y una función de control. Y es así como la vieja red se emplea a gran escala.

Los primeros sistemas que alcanzan un desarrollo comercial significativo aparecen en los años ochenta: En Europa los sistemas NMT-450 y en EE.UU., el sistema AMPS- "American Mobile Phone System" adaptado en Europa como TACS "Total Access

Communication System" empiezan ofreciendo un servicio que tiene, desde el punto de vista de usuario, las características del servicio actual:

1. Posibilidad de realizar y recibir llamadas en cualquier punto del área de cobertura del sistema.

2. Continuidad de la comunicación al pasar del radio de acción de una estación de base al de la estación contigua.

Sin embargo, estos sistemas solo alcanzan unas penetraciones limitadas debido a los elevados costos que implican. Solo en los países nórdicos, en los que las condiciones económicas (altos ingresos percapitas, sociales y tendencia a vivir en el campo) eran particularmente favorables, se llega a una amplia penetración.

¿Cuáles son las razones de que los costos fueran tan elevados? Las hay de dos tipos:

a) Por un lado, falta de competencia entre los operadores y suministradores de equipos que obligaran a bajar los precios. Cuando en Gran Bretaña se introdujo el segundo operador, incluso el crecimiento del sistema TACS, analógico, se acelero considerablemente.

b) Por otro, dificultades de orden técnico. Entre estas las más destacables son:

- Existencia de varios estándares y, por tanto, series de fabricación limitadas.

- Sistemas de baja capacidad o eficiencia radioeléctrica que implica un gran consumo de frecuencias o bien instalaciones caras.

- Sistemas analógicos que implican una tecnología voluminosa y de difícil mantenimiento.

- Sistemas propietarios, es decir, dependencia de un único fabricante.

Esta primera generación de telefonía móvil hizo su aparición en 1979, y se caracterizó por ser analógica y estrictamente para voz.

La calidad de los enlaces de voz era muy baja, baja velocidad (2400 bauds), la transferencia entre celdas era muy imprecisa, tenían baja capacidad (basadas en FDMA, “Frequency Divison Multiple Access”) y la seguridad no existía. La tecnología predominante de esta generación es AMPS “Advanced Mobile Phone System”.

Los dispositivos eran muy pesados y de gran tamaño, debido a que tenían que realizar una emisión de gran potencia para poder lograr una comunicación sin cortes ni interferencias. La batería no era muy eficiente en el almacenamiento de la carga, además de ser enorme.

El siguiente cuadro muestra algunos sistemas de telefonía celular empleados durante la primera generación:

Tabla 3.1 Sistemas de telefonía celular de la primera generación

Sistema	**País**	**No. Canales**	**Espacia (kHz)**
AMPS	EE.UU.	832	30
C-450	Alemania	573	10
ETACS	Reino Unido	1240	25
JTACS	Japón	800	12.5
NMT-900	Escandinavia	1999	12.5
NMT-450	Escandinavia	180	25
NTT	Japón	2400	6.25
Radiocom-200	Francia	560	12.5
RTMS	Italia	200	25
TACS	Reino Unido	1000	125

AMPS

Desarrollado por los Laboratorios Bell AT&T. Funciona en la banda de los 800 MHz.

EAMPS

“Extended AMPS” (AMPS extendido). Aumenta la capacidad del AMPS y aun hoy en día continúa siendo el sistema mas extendido en EE.UU. y su entorno de influencia.

NAMPS

“Narrowband AMPS” (AMPS de banda estrecha). Desarrollado por Motorola a partir del EAMPS, siendo un sistema a medio camino entre el analógico y el digital.

C-450

Sistema sudafricano (nada menos) ahora conocido por “Motorphone System 512”. Y aún sigue en funcionamiento, solo en Sudáfrica.

C-Netz

Antiguo sistema que funcionaba en la banda de 450 MHz usado en Alemania y Austria.

Comvik

Otra victima de la estandarización con la llegada del GSM, nació en Suecia en 1981 y pasó a mejor vida en 1996.

NMT 450

“Nordic Mobile Telephones” Sistema Nórdico de Telefonía Móvil, desarrollado por Nokia y Ericsson para entornos nórdicos, funcionaba a 450 MHz: También se implanto en España, durante los '80, por la operadora MoviLine.

NMT 900

El sistema NMT “Nordic Mobile Telephony” surgió en los países escandinavos en 1981, es ideal para cubrir la mayor extensión de terreno con la menor inversión. Esta versión NMT 900 permite un mayor número de canales. Heredero del anterior, empleaba la banda

de 900 MHz, para permitir mayor capacidad y terminales más pequeñas.

NMT-F

Versión francesa del anterior.

NTT

“Nippon Telegraph & Telephone”. Desarrollado por la empresa telefónica japonesa, ha sido el estándar analógico en esta zona. Apareció una versión de alta capacidad llamada HICAP.

RC2000

Radiocom 2000. Sistema francés que entró en funcionamiento a finales de 1985.

TACS

“Total Access Communications System”. Se desarrolló en Inglaterra el año 1985 por parte de Motorola, operando en la banda de 900 MHz. El sistema TACS 900 adaptado, deriva del sistema analógico AMPS americano desarrollado por los laboratorios Bell y comercializado en EE.UU en 1984. Con este sistema se obtiene una mejor calidad del servicio, al mismo tiempo que mejora la relación señal/ruido por tener una mayor anchura de canal. Además precisa de equipos más pequeños y baratos.

El sistema TACS (Total Access Communications System) 900 conocido como TMA 900, es del mismo tipo que el anterior, analógico multicanalizado en frecuencia, pero diferente por utilizar una tecnología mucho más avanzada y barata, dando mejor calidad de

audio, así como una mejor conmutación al pasar de una a otra célula, ya que la señalización se realiza fuera de banda, al contrario que NMT, que lo hace dentro de ella, resultando casi imperceptible el ruido para el usuario, sin embargo sus estaciones base cubren un intervalo menor. Emplea la banda de frecuencia de los 900 MHz y cada MHz se divide en 40 semicanales de 25 kHz, por lo que resulta extremadamente útil, por su gran disponibilidad de canales, para cubrir áreas urbanas. Dispone de 1320 canales duplex, de los que 21 se dedican exclusivamente a control (señal digital) y el resto para voz (señal analógica)

ITACS

"International TACS". Versión mejorada del TACS con un sistema de control mejorado.

ETACS

"Extended TACS". Sustituto del TACS.

JTACS

"Japan TACS". Es una versión del TACS desarrollada especialmente para Japon.

IETACS

"International ETACS". Una variación menor del ETACS, que aporta más flexibilidad.

NTACS

"Narrowband TACS", TACS de banda estrecha. Triplica la capacidad del ETACS sin pérdida de calidad de la señal.

3.2.2 CÁLCULO DE DIMENSIONAMIENTO EN SISTEMAS DE PRIMERA GENERACIÓN

En los sistemas de “trunking” se efectúa el dimensionamiento en función del grado de servicio (GOS), definido como `producto de la probabilidad de espera por la probabilidad de que el tiempo de espera supere un valor dado. Generalmente este valor es la duración media de la llamada. Se aplica la distribución Erlahg C convencional.

Para los sistemas públicos celulares que trabajan en régimen de llamadas perdidas, el procedimiento es similar, en principio al que se aplica en las redes de telecomunicaciones convencionales. Ahora bien deben considerarse algunos efectos propios de la movilidad de las terminales como son:

- Acortamiento de la duración media de la llamada percibida desde la estación base, pues algunos móviles abandonarán la celda en el curso de la llamada.
- Aumento de la tasa efectiva de llamadas entrantes para los móviles que acceden a la celda con una llamada en curso.
- Interrupción forzada y prematura de algunas llamadas cuando, al efectuarse la transferencia a una celda vecina, no hay en ésta canales libres.

Por lo que, la metodología que puede seguirse para el dimensionamiento, según una estrategia de asignación fija de los recursos, en la cual se asigna de modo permanente un juego de

canales a cada celda, el cual repite al cabo de la distancia de reutilización.

Con esta estrategia cada llamada se cursa a través de alguno de los radiocanales libres de la celda. Si están todos ocupados, la llamada se pierde.

Puede aumentarse el número de móviles o reducirse la tasa global de bloqueo, haciendo uso de una estrategia de asignación dinámica, en virtud de la cual una celda con todos sus radiocanales ocupados puede pedir prestadas una o más frecuencias a alguna de sus células vecinas con el fin de satisfacer una petición de comunicación en su ámbito.

3.3 SEGUNDA GENERACIÓN DE TELEFONÍA CELULAR

La segunda generación 2G arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad. Las tecnologías predominantes son:

- GSM Sistema Global para Comunicaciones Móviles. “Global System for Mobile Communications”,
- IS-136 conocido también como TIA/EIA-136 o ANSI-136. Éstos dos primeros basados en TDMA.
- IS-95 basado en CDMA Código de división múltiple de acceso “Code Division Multiple Access” y
- PDC Comunicaciones Digitales Personales “Personal Digital Communications”.

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (Servicio de Mensajes Cortos “Short Message Service”). La mayoría de los protocolos de segunda generación ofrecen diferentes niveles de encriptación. En los Estados Unidos y otros países se le conoce a éstos como PCS (Servicios de Comunicaciones Personales “Personal Communications Services”).

La principal ventaja de los teléfonos de segunda generación sobre sus precesores analógicos son su gran capacidad y menor necesidad de carga de batería. En otras palabras, ellos satisfacen a los usuarios asignando una frecuencia consumiendo menos potencia.

3.3.1 GENERACIÓN 2.5G

La generación 2.5G ofrece características extendidas para ofrecer capacidades adicionales que los sistemas segunda generación tales como GPRS “General Packet Radio System”, HSCSD “High Speed Circuit Switched Data”, EDGE “Enhanced Data Rates for Global Evolution”, IS-136B, IS-95B, entre otros. La tecnología 2.5G es más rápida y más económica para actualizarse a los sistemas de tercera generación.

Muchos de los proveedores de servicios de telecomunicaciones (“carriers”) se moverán a las redes 2.5G antes de entrar masivamente a 3G. Los “carriers” europeos y de Estados Unidos se moverán a 2.5G en el 2001. Mientras que Japón ira directo de 2G a 3G también en el 2001.

3.3.2 SISTEMA GSM

A partir de 1982, en el seno de la CEPT “Conférence Européenne des Administrations des Postes et des Télécommunicarions”, se vio la necesidad de comenzar tareas de planificación de un nuevo sistema de comunicaciones móviles, posteriormente conocido como GSM, que sustituyera a los sistemas analógicos por digitales.

El sistema GSM se planteó como un sistema multioperador. El estándar fue diseñado con la posibilidad de que varios operadores pudieran compartir el espectro. Funciona a frecuencias de 900 MHz.

El rápido crecimiento de los sistemas celulares, así como razonables socioeconómicas junto con el problema de la falta de frecuencias de 900 MHz, impulso una adaptación del sistema GSM a la banda de 1800 MHz (1900 en EE.UU.). Este sistema se denomina DCS-1800. En realidad, DCS pude considerarse como una variante de GMS que resuelve su problema más acuciante: la falta de espectro para planificar de forma económica las áreas urbanas.

3.3.3 COBERTURA EN LOS SISTEMAS 2G

Como los tamaños de las celdas son cada vez más reducidos, pasando de miniceldas de 2Km (GSM) a microceldas de unos 500m (DCS-1800) y picoceldas de 50m (DECT), es necesario mejorar la precisión de las predicciones. En efecto, un error de cálculo de cobertura de 100m puede ser admisible en una minicelda, pero no en una picocelda. Por otro lado, se exige la cobertura en entornos especiales: túneles viarios, estacionamientos subterráneos, interiores de edificios,

etc., lo que conlleva la caracterización de estos nuevos entornos. También adquiere cada vez más importancia la caracterización del canal en banda ancha para la optimización de la operación. Debe subrayarse que los operadores, una vez superada la fase de despliegue de la red móvil, deben consolidar sus objetivos de calidad-cobertura, con un análisis más detallado de las perturbaciones para compensar sus efectos y mejorar la calidad de las telecomunicaciones.

Una solución que se esta estudiando activamente es la que emplea la Teoría Geométrica de la Difracción (GTD) y Teoría Uniforme de la Difracción (UTD), tanto en forma bidimensional (2D) y tridimensional (3D), combinada con modelos de dispersión radar y linealización de perfiles. Son de destacar también los nuevos métodos de predicción basados en redes neuronales combinados con medidas.

Asimismo, se empiezan a utilizar bases de datos digitales de ciudades para aplicar los más detallados modelos urbanos, tanto en banda estrecha, para el cálculo de la pérdida básica de propagación, como en banda ancha.

3.4 TERCERA GENERACIÓN DE TELEFONÍA CELULAR

El propósito de la Tercera generación (figura 3.1) consiste en superar las limitaciones técnicas de las tecnologías precedentes. La tercera generación es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos.

Los protocolos empleados en los sistemas 3G soportan altas velocidades de información enfocados para aplicaciones mas allá de la voz tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet, sólo por nombrar algunos.

Entre las tecnologías contendientes de la tercera generación se encuentran UMTS “Universal Mobile Telephone Service”, CDMA2000, IMT-2000, ARIB (3GPP), UWC-136, entre otras.

El impulso de los estándares de la 3G está siendo apoyando por la Unión Internacional de Telecomunicaciones ITU “International Telecomunications Union” y a este esfuerzo se le conoce como IMT-2000 Telecomunicaciones Móviles Internacionales para el año 2000 “International Mobile Telephone”.

Los principales requerimientos para esta tecnología incluyen:

- Calidad de voz comparable a la que ofrece una red telefónica pública (PSTN).
- Velocidades de transmisión de datos de 144kb/s para usuarios en vehículos en movimiento viajando a una velocidad de 120Km/h en ambientes exteriores.
- Velocidades de transmisión de datos de 384kb/s para peatones, que se encuentren en un solo lugar o bien moviéndose sobre áreas pequeñas.
- Soporte para operaciones de 2.048 Mb/s en oficinas, es decir en ambientes estacionarios de corto alcance o en interiores.
- Soporte para ambos servicios de datos conmutación por paquetes y conmutación por circuitos.

- Una interfaz adaptada para las comunicaciones móviles de Internet., que permita un ancho de banda más grande para enviar información que para recibir.
- Mayor eficiencia del espectro disponible.
- Soporte para una gran variedad de equipo móvil.
- Introducción flexible a los nuevos servicios y tecnologías.

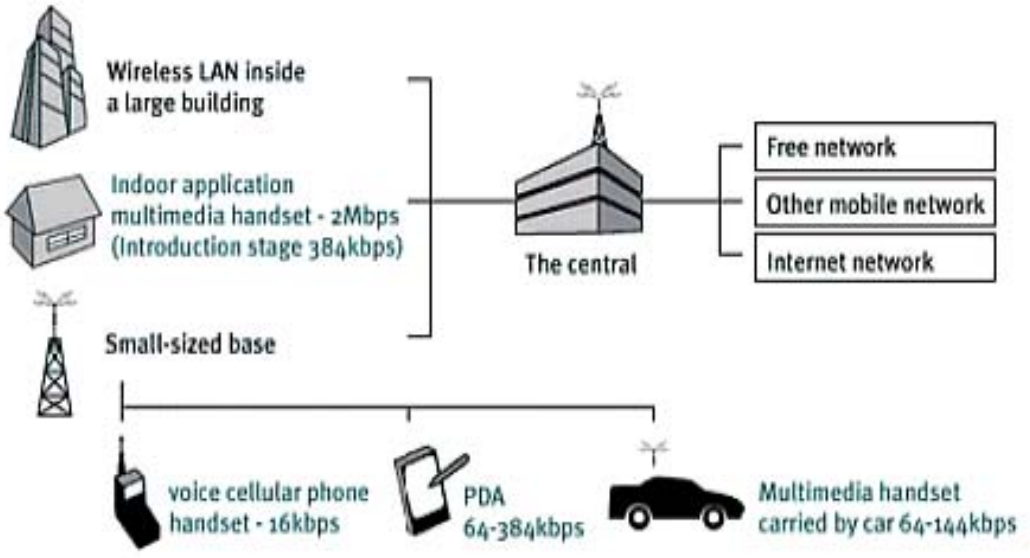

Figura 3.1 Tercera generación Fuente: www.monografias.com

Lo ideal es que los sistemas de tercera generación provean servicios en cualquier lugar y a cualquier hora. Mientras que los servicios analógicos y los primeros servicios digitales fueron diseñados solo para resolver problemas de sistemas analógicos, como seguridad, bloqueo e incompatibilidad regional; iniciándose así, una nueva visión a la migración a 3G y por lo tanto hacia nuevos servicios.

Actualmente solo diez de las tecnologías de transmisión de radio terrestre (RTTs) tienen los mínimos requerimientos de capacidad de IMT-2000 presentado por la ITU en junio de 1998. Éstas se muestran a continuación.

Una de las propuestas más prometedoras para la creación de la nueva generación es la combinación de la interfaz aérea del ancho de banda de CDMA (W-CDMA) con la red GSM.

Entre las diversas organizaciones que procuran combinar sus ofertas de W-CDMA están la Asociación de Japón de las Industrias y de los Negocios de Radio (ARIB), la Alianza para las Soluciones de la Industria de las Telecomunicaciones (ATIS), T1P1, Los Servicios sin hilos Integrados de la Red Digital de Multimedia (WIMS), y el Instituto Europeo de Estandarización de Telecomunicaciones (ETSI) a través de su Grupo Móvil Especial (GMS). El esquema que tienen en mente se aprovecha de las técnicas de radio de W-CDMA sin hacer caso de los numerosos sistemas desplegados por GSM.

Estas organizaciones se basan en el Sistema Móvil Universal de Telecomunicación (UMTS) de ETSI´s. Llamado UTRA (para el acceso de radio terrestre de UMTS), la propuesta describe dos modos de funcionamiento: el multiplexaje de la frecuencia y de división de tiempo.

3.4.1 PROPUESTA CDMA2000 PARA REVESTIR IS-95

El subcomité TR-45.5 de la Asociación de la Industria de Telecomunicaciones (TIA) sometió una tecnología de radio de

transmisión llamada CDMA2000. Este RTT protege inversiones en el equipo y los sistemas IS-95, de los cuales existen varios en Norteamérica y Corea.

La tecnología propuesta explota al máximo la capacidad del sistema de segunda generación actual de CDMA para validar algunas características de la tercera generación. De hecho, los sistemas actuales, conocidos como CDMAOne, se pueden ver como versiones de banda estrecha de sistemas completamente desarrollados para la tercera generación CDMA2000.

La tecnología TR45.5 utiliza “handoffs” entre los sistemas de segunda generación (CDMAOne) y de tercera generación (CDMA2000) así como ambas técnicas de radio de división de en dos canales de frecuencia y de tiempo. Un sistema de CDMAOne puede desplegar algunas características de la nueva generación sin ampliar el ancho de banda del canal, a condición de que ciertos detalles de señalización y de recursos lógicos dentro del canal 1.25-MHz que se modifican para resolver las necesidades del paquete de la radio y de servicios asimétricos. Más características de banda ancha pueden ser agregadas más adelante multicanalizando los canales adicionales de CDMAOne en incrementos de 1,25 MHz.

3.4.2 UMTS

UMTS “Universal Mobile Telephone Service” es un sistema móvil de tercera generación que está siendo desarrollado por el organismo ETSI (European Telecommunications Standards Institute) junto el IMT-2000 de la ITU. UMTS es sistema europeo que está intentando

combinar la telefonía celular, teléfonos inalámbricos, redes locales de datos, radios móviles privados y sistemas de radiolocalización “paging”. Que va a proveer velocidades de hasta 2 Mbps, haciendo los videoteléfonos una realidad. Las licencias de UMTS están atrayendo gran interés entre los “carriers” del continente europeo debido a que representa una oportunidad única para crear un mercado en masa para el acceso a la información, altamente personalizado y amigable para la sociedad. UMTS busca cimentar y extender el potencial de las tecnologías móviles, inalámbricas y satelitales de hoy en día.

3.4.3 PROYECCIÓN DE LA 3G

Lo que sigue en este momento es esperar a que los “carriers” ofrezcan los servicios de 3G. Por ejemplo, en Japón ya están operando con las tecnologías de 3G. El servicio con más éxito es “i-mode” de NTT DoCoMo que utiliza una red basada en paquetes conocida como PDC-P, aunque es una tecnología propietaria que tiene actualmente más de 17 millones de subscriptores. NTT DoCoMo también piensa incursionar con W-CDMA y sus contendientes en ese país para servicios 3G son DDI y J-Phone. En Estados Unidos, compañías como Qualcomm y Sprint PCS ya empezaron a realizar pruebas del servicio 3G.

La batalla por las licencias de 3G de UMTS es otro asunto de gran importancia y varias son las compañías las involucradas en obtener las valiosas licencias de telefonía móvil de tercera generación, tales como: Telecom Italia (Italia); Vodafone, Orange y BT Cellnet (Inglaterra); T-Mobil (Alemania), France Telecom (Francia); KPN

Telecom (Holanda), NTTDoCoMo (Japón), etc. Las compañías que dominan mercados pequeños deberán aliarse con los grupos grandes.

A parte de las cantidades enormes de dinero que cuestan las licencias, hay que tomar en cuenta que las redes telefónicas de estos "carriers" son redes grandes y complejas, por lo que les tomará tiempo y grandes inversiones de capital para implantar la tecnología. Pero muchas de las ventajas de esas redes son que varias de ellas ya están ofreciendo servicios de datos, y prevalecerán aquellas empresas de telecomunicaciones que tengan la mayor experiencia en tecnologías inalámbricas y tomen ventaja de ello para las nuevas redes del futuro.

En relación en predicciones en cuanto a usuarios móviles, "The Yankee Group" anticipa que en el 2004 habrá más de 1150 Millones de usuarios móviles en el mundo, comparados con los 700 millones que hubo en el 2000. Por otra parte Ericsson predice que habrá 1000 millones de usuarios en el 2002. Dichas cifras nos anticipan un gran numero de capital involucrado en la telefonía inalámbrica, lo que con más razón las compañías fabricantes de tecnología, así como los proveedores de servicios de telecomunicaciones estarán dispuestos a invertir su capital en esta nueva aventura llamada 3G.

Independientemente de cual tecnología en telefonía inalámbrica predomine, lo único que le interesa al usuario final es la calidad de voz, que no se bloqueen las llamadas y que en realidad se ofrezcan las velocidades prometidas. El tiempo y las fuerzas del mercado nos darán la razón.

3.5 ¿CÓMO FUNCIONA?

Tal como otros aparatos en nuestra vida cotidiana, un teléfono celular es un verdadero misterio para la mayoría de las personas y en ocasiones no imaginamos lo que hay dentro de él. Si destapamos nuestro aparato celular encontraremos lo siguiente:

- Circuito integrado que contiene el cerebro del teléfono.
- Antena.
- Pantalla de cristal líquido (LCD).
- Teclado pequeño.
- Micrófono.
- Bocina.
- Batería.

Un teléfono móvil utiliza dos frecuencias diferentes: una para transmitir y otra para recibir, permitiendo una conversación normal.

3.5.1 CÉLULAS

Antes de la invención de las células, se usaban radioteléfonos que transmitían hacia una antena central en cada ciudad con 25 canales disponibles. Las desventajas de este sistema eran que exigían transmisores muy potentes, o al menos, lo suficiente para transmitir a 60 o a 80 km. Esto implicaba un sistema muy caro y frecuencias insuficientes.

En las décadas de los 70´s y los 80´s fue inventado el sistema de células (figura 3.2). Una célula es un área determinada, pequeña, que

tiene las ventajas de requerir transmisores mucho menos potentes que uno del sistema anterior y el uso extensivo de frecuencias en todas las ciudades, a través de la reutilización.

Esto se realiza a través del reparto de una zona en varias células (áreas más pequeñas), de forma hexagonal, para poder abarcar todo el espacio. En cada célula existe una estación base transmisora, con lo cual, se pueden tener múltiples canales para el uso de decenas de celulares de manera simultánea. Cuando un usuario pasa de una célula a otra deja la frecuencia que estaba utilizando, para el uso de otro celular, y toma la frecuencia libre de la célula a la que pasó.

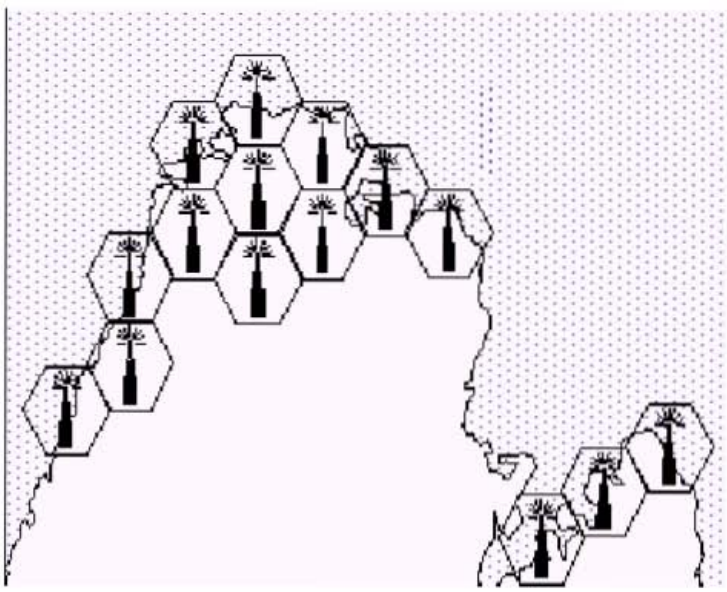

Figura 3.2 Células Fuente: www.monografias.com

Como las distancias de transmisión no son muy grandes, los teléfonos móviles pueden transmitir con poca energía; por lo tanto, con

pequeñas baterías que permiten un tamaño y peso reducido. Por lo anterior, es que son usadas las células en la telefonía celular.

3.5.2 HANDOFF

La transición del enlace de comunicación de una estación base a otra, aledaña, se conoce como “handoff” (figura 3.3)

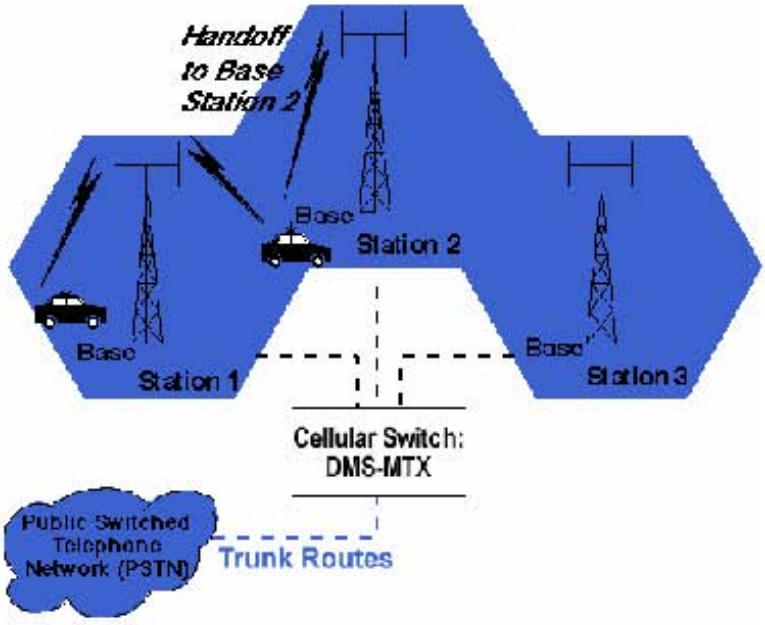

Figura 3.3 Handoff Fuente: www.monografías.com

El sistema CDMA define diferentes procesos de “handoff”, que se explican a continuación.

El primero es el “soft handoff” o “handoff de software”. Durante el “handoff”, un móvil mantiene, simultáneamente, conexión con dos o

tres estaciones base. Cuando el móvil se mueve de su célula actual (Fuente) a la siguiente célula (objetivo), siempre se mantiene una conexión de canal de tráfico con ambas células. En el enlace de bajada, el móvil usa el receptor múltiple o “rake receiver” para demodular dos señales separadas de dos estaciones base diferentes. Las dos señales se combinan para obtener una señal compuesta de mejor calidad. En el enlace de subida, la señal que transmite el móvil se recibe por ambas estaciones base. Las dos células demodulan la señal por separado y envían las tramas demoduladas al centro de conmutación móvil (MSC, “mobile switching center”). El MSC contiene un selector que obtiene la mejor trama de las dos.

El segundo es el “softer handoff”. Este tipo de “handoff” ocurre cuando un móvil hace una transición entre dos sectores de la misma célula. En el enlace de bajada, el móvil mejora la misma clase de combinación de proceso que el “soft handoff”. En este caso, el móvil usa su receptor múltiple para combinar las señales recibidas de los dos sectores. En el enlace de subida, sin embargo, dos sectores de la misma célula reciben simultáneamente las dos señales del móvil. Estas señales son demoduladas y combinadas dentro de la célula, de tal forma que únicamente se envía una trama al MSC.

El tercero es el “hard handoff” o “handoff de hardware”. El sistema CDMA hace dos tipos de “hard handoffs”. Un “handoff CDMA-a-CDMA” ocurre cuando el móvil hace una transición entre dos portadoras CDMA (por ejemplo, dos canales de espectro esparcido que están centrados en diferentes frecuencias). Este “hard handoff” ocurre también cuando el móvil hace una transición entre dos sistemas diferentes de operadores. Al “handoff CDMA-a-CDMA” también se le

llama “D-a-D handoff”. Y el “handoff CDMA-a-analógico” ocurre cuando una llamada CDMA se guía a una red analógica. Esto puede ocurrir cuando el móvil viaja en un área donde hay servicio analógico pero no hay servicio CDMA. El “handoff CDMA-a-analógico” se le llama “handoff D-a-A”.

Antes de describir el proceso de “soft handoff” en detalle, es importante notar que cada sector en un sistema CDMA se distingue de cualquier otro por su canal piloto. El canal piloto es uno de los cuatro canales -piloto, ‘paging’, ‘sync’ y canales de tráfico- en el enlace de bajada. El canal piloto sirve como un "faro" para el sector y ayuda al móvil a adquirir otros canales lógicos del sector. El piloto no contiene información más que en el código corto PN (“Pseudo Noise” o de pseudo ruido).

Se usa un término especial para describir la SNR del canal de piloto: energía por chip por densidad de interferencia, o E_c/I_0. La energía por chip E_c/I_0 es diferente de la energía por bit E_b en que "chips" se refiere a los bits en las secuencias esparcidas PN. Dado que no hay información en banda base contenida en el canal de piloto, el piloto no pasa por el proceso opuesto al esparcimiento y estos bits no se recobran.

El móvil constantemente notifica a la estación base las condiciones de la propagación local; la estación base hace uso de esta información para tomar decisiones sobre el “handoff”. Este “handoff” asistido del móvil (MAHO, “mobile-assisted handoff”) actúa cuando el móvil toma una medida del E_c/I_0 del enlace de bajada y reporta el resultado de la medida a la estación base. Dado que cada estación base transmite su

propio piloto en un diferente “offset” PN, el E_c/I_0 de un piloto da una buena indicación de sí un sector en particular puede o no ser el sector más apropiado para servir al móvil.

En el manejo del proceso de “handoff”, el móvil mantiene en su memoria cuatro listas que se excluyen entre sí compuestas por los sectores de las estaciones base. A estas listas también se les llama conjuntos. Los cuatro conjuntos son conjunto activo (“active”), conjunto candidato (“candidate”), conjunto vecino (“neighbor”), y conjunto residuo (“remaining”).

El conjunto activo contiene los pilotos de aquellos sectores que se están comunicando con el móvil en los canales de tráfico. Si el conjunto activo contiene únicamente un piloto, entonces el móvil no está en “soft handoff”. Si el conjunto activo contiene mas de un piloto, entonces el móvil mantiene la conexión con todos esos sectores en canales de tráfico separados. La estación base controla esencialmente el proceso de “handoff” porque se puede agregar únicamente un piloto al conjunto activo si la estación base envía un “mensaje de dirección de handoff” (“handoff direction message”) al móvil y el mensaje contiene el piloto en particular
que se va a agregar al conjunto activo. El conjunto activo puede contener a lo más seis pilotos.

El conjunto candidato contiene aquellos pilotos cuyos E_c/I_0 son suficientes para hacerlos candidatos de handoff. Esto significa que si el E_c/I_0 de un piloto en particular es más grande que el umbral de detección de piloto (“pilot detection threshold”) “T_ADD”, entonces

ese piloto se agrega al conjunto candidato. El conjunto candidato solo puede contener seis pilotos.

El conjunto vecino contiene aquellos pilotos que están en la lista vecino del actual sector servidor del móvil. El conjunto vecino contiene a lo mas 20 pilotos.

El conjunto residuo contiene todos los posibles pilotos en el sistema para esta frecuencia portadora, excluyendo a los pilotos que están en los conjuntos activo, candidato y vecino.

3.6 PROCESO

A continuación se muestra el proceso que sigue una llamada para entrar en “hand off”, (ver figura 3.4) mostrando la importancia de la función que tiene que cumplir ambas células (fuente y objetivo).

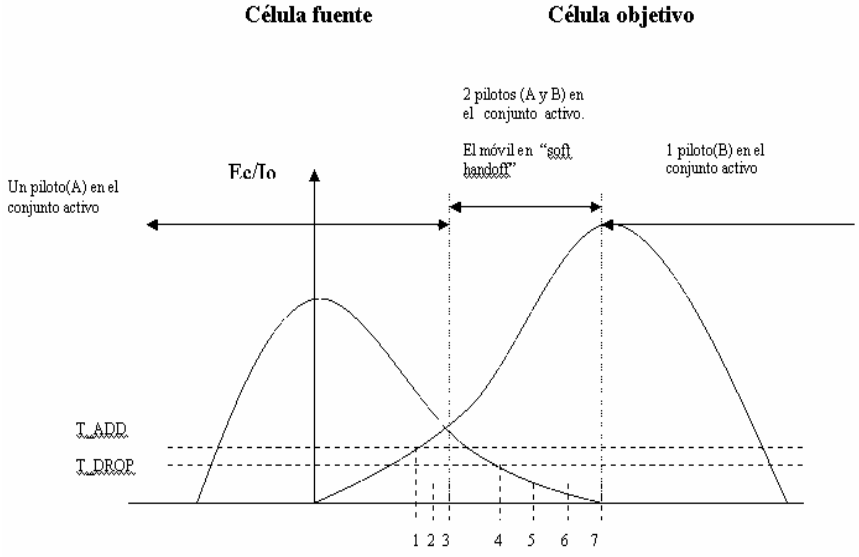

Figura 3.4 Proceso de una llamada Fuente: www.google.com

1. En primera instancia el móvil se encuentra alimentado únicamente por la célula Fuente, y su conjunto activo contiene tan solo al piloto A(célula Fuente). El móvil mide el nivel de E_c/I_0 del piloto B(célula objetivo) y si lo encuentra mayor que “T_ADD”, el móvil envía un mensaje de medida de fuerza de piloto (“pilot strength measurement message”) y transfiere al piloto B del conjunto vecino al conjunto candidato.
2. Ahora el móvil recibe un “mensaje de dirección de handoff” (“handoff direction message”) de la célula Fuente. Dicho mensaje ordena al móvil a comenzar la comunicación en un nuevo canal de tráfico con la célula objetivo. El mensaje contiene el “PN offset” de la célula objetivo y el código de Walsh del nuevo canal de tráfico.
3. Entonces el móvil mueve el piloto del conjunto candidato al conjunto activo. En este momento el móvil envía un “mensaje de acabado de handoff” (“handoff completion message”) inmediatamente después de adquirir el canal de tráfico de bajada especificado en el “mensaje de dirección de handoff” (“handoff direction message”). Ahora el conjunto activo contiene dos pilotos en su lista.
4. Después de que tiene dos pilotos, el móvil detecta que el piloto A ha caído por debajo de “T_DROP” y es entonces cuando el móvil inicia el contador de tiempo o “drop timer”.
5. Cuando el “drop timer” alcanza el valor correspondiente a “T_TDROP” el móvil envía un mensaje de medida de fuerza de piloto (“pilot strength measurement message”).

6. Una vez que el móvil recibe un “mensaje de dirección de handoff”, el mensaje contiene únicamente el PN offset de la célula objetivo.
7. Y finalmente el móvil tiene que cambiar el piloto Fuente del conjunto activo al conjunto vecino, así como enviar un mensaje para indicar que el “handoff” ha terminado.

3.6.1 FRECUENCIA DE REUSO

El sistema AMPS uso el concepto de la frecuencia de reuso en las comunicaciones celulares, donde, el número total de células son divididas dentro de “clusters” y cada célula dentro del “cluster” le será asignada frecuencias las cuales son distintas y no interfieren con las frecuencias de las células adyacentes.

El mismo patrón de asignamiento de canales es repetido en los “clusters” adyacentes. En tamaño mínimo de un “cluster” (N) fue determinado de acuerdo a las condiciones de interferencia co-canal y fue directamente relacionado a una parámetro llamado la relación d/r, donde ‘d’ es la distancia entre las células las cuales reusan los mismos canales y ‘r’ es el radio de la célula. Un valor de d/r = 4.6 fue encontrado adecuado para antenas direccionales y D/R de 6.0 fue requerido para antenas omnidireccionales para mantener una relación señal a ruido de 17 dB requerida para una buena calidad de trasmisión. Esto corresponde a una valor de N = 7 (para antenas direccionales) y N = 12 (para antenas omni-direccionales) el cual fue utilizado cono el tamaño de un “cluster” en el sistema AMPS.

3.6.2 DIVISIÓN DE CÉLULA

En áreas donde la densidad de tráfico es muy alta, nuevas células pueden ser agregadas entre los sitios de células ya existentes para obtener un nuevo patrón de células con la mitad de dimensión lineal que los sitios de células originales. La división de células en este patrón incrementa el número de canales, desde que las células pequeñas pueden aguantar muchos canales y largos, manteniendo la misma relación d/r. Asignando apropiadamente las frecuencias de radio de canal, en sistema AMPS puede permitir la coexistencia de células largas y pequeñas. Cuando el crecimiento de un cliente se incrementa, las células pequeñas pueden ser subdivididas mas para incrementar la capacidad del sistema. La eficiencia del espectro fue alcanzada en el sistema AMPS por este método bajo el costo del incremento el número de sitios de células requeridos para un área particular.

3.7 EL PAPEL DE BLUETOOTH

La aplicación Bluetooth está abriendo las puertas a nuevas aplicaciones para extender el papel de la telefonía móvil más allá del servicio de telefonía convencional en nuestros dias. De hecho, la viabilidad comercial de los nuevos desarrollos podría perfectamente depender bien de la capacidad de la tecnología Bluetooth para soportar mecanismos de comunicación inalámbrica tales como la telefonía celular. Mientras las redes sean adecuadas para establecer comunicaciones móviles o proporcionar acceso inalámbrico a cualquier lugar, la interconexión solamente local se gestiona mejor mediante un

sistema multipropósito como el proporcionado por la especificación Bluetooth.

La tercera generación celular ha sido diseñada para llevar paquetes de datos y la comunicación de voz es tratada simplemente como otra aplicación de datos. La especificación Bluetooth soporta tanto sistemas 2G mejorados como sistemas 3G para la provisión de un amplio rango de servicios, desde redes LAN y WAN a equipos PDA.

La tecnología inalámbrica Bluetooth puede interconectar simultáneamente hasta ocho dispositivos en una picorred de corto alcance, entonces varias picorredes pueden operar en las proximidades y los dispositivos Bluetooth pueden moverse rápidamente de una picorred a otra. De hecho los dispositivos Bluetooth solamente necesitan permanecer como miembros de una picorred durante el período de tiempo requerido para completar una transacción de comunicación. También los dispositivos pueden unirse a una picorred y abandonarla rápida y frecuentemente, superando en la práctica el límite de los ocho dispositivos.

Los dispositivos Bluetooth que no forman actualmente parte de una picorred están escuchando constantemente a los otros dispositivos Bluetooth; cuando están lo suficientemente próximos como para formar parte de la picorred, se identifican a sí mismos de manera que los otros dispositivos pueden comunicarse con ellos si lo necesitan.

Otra característica de los dispositivos es que pueden admitir múltiples conexiones de datos y hasta tres conexiones de voz simultáneamente,

proporcionando la funcionalidad de un sistema multimedia intercomunicador de tres microteléfonos inalámbricos. El límite de tres terminales interconectados se aplica específicamente a la conversación; el límite para el número de terminales intercambiando datos sería de ocho por picorred.

Por lo tanto, de esta manera resalta la funcionalidad complementaria de Bluetooth y los sistemas celulares 3G. El sistema 3G se utiliza para proporcionar conexión con un ligar específico, mientras que la tecnología inalámbrica Bluetooth se emplea para la distribución final de la información de los dispositivos locales. De esta manera se reduce considerablemente la cantidad de tráfico innecesario a través de la red 3G, creando una solución efectiva en términos de costo.

Las siguientes fotografías (figura 3.5 y 3.6) son una pequeña muestra de la gran diversidad de celulares GSM existentes en el mercado tecnológico, adicionados con bluetooth en la actualidad.

Figura 3.5 Celulares GSM Fuente: www.google.com

Figura 3.6 Celulares GSM Fuente: www.google.com

CAPÍTULO IV. SEGURIDAD EN BLUETOOTH

Las señales Bluetooth pueden ser interceptadas fácilmente, como cualquier otro tipo de señal inalámbrica. Por lo tanto, la especificación Bluetooth requiere de una integración de mecanismos de seguridad para prevenir los intentos de falsificar el origen de los mensajes, a lo cual, se le denomina suplantación. En si, hay disponibles características de seguridad de nivel de enlace que emplean mecanismos de autenticación y cifrado.

La autenticación previene la suplantación y los accesos no deseados a datos y funciones críticas, mientras que el cifrado protege la confidencialidad del enlace.

4.1 MODOS DE SEGURIDAD

El modo 1 hace referencia a la ausencia de seguridad y es utilizado cuando los dispositivos no tienen aplicaciones críticas. En este modo, los dispositivos desactivan las funciones de seguridad de nivel de enlace, siendo útiles para acceder a bases de datos que contengan información no sensible.

El modo 2 proporciona seguridad de nivel de servicio, permitiendo procedimientos de acceso más versátiles, en especial para aplicaciones que se ejecuten en paralelo.

Además, en este modelo es posible definir niveles de seguridad. Los dispositivos tienen dos niveles de confianza, los cuales determinan el

nivel de acceso a los servicios. Un dispositivo de confianza es uno que tiene una relación fija (emparejamiento) y goza de acceso sin restricciones a todos los servicios.

Un dispositivo no confiable es aquel que no tiene ninguna relación fija permanente, por lo tanto, no es de confianza.

El modo 3 proporciona seguridad de nivel de enlace, donde el gestor de enlace (LM) impone una seguridad de nivel común para todas las aplicaciones en el momento de configurar la conexión. Este modo obliga a un nivel de seguridad común y es más fácil de implementar que el modo 2.

4.2 SEGURIDAD DE NIVEL DE ENLACE

Las funciones de seguridad de nivel de enlace están basadas en el concepto de claves de enlace, los cuales son números aleatorios de 128 bits almacenados individualmente para cada par de dispositivos. La autenticación consiste en un esquema de desafío/respuesta entre cada par de dispositivos que emplea una clave de enlace secreta común de 128 bits, un desafío de 128 bits y una respuesta de 32 bits. Este esquema se emplea para autenticar dispositivos, no usuarios.

Cada que dos mismos dispositivos se comunican a través de un dispositivo Bluetooth, se utiliza la clave de enlace para autenticación y cifrado, sin importar la topología de la picorred. El tipo más seguro de clave de enlace es una clave combinada, la cual es obtenida mediante

los datos proporcionados por ambos dispositivos. Otra opción es elegir una clave de unidad, la cual es recomendada para dispositivos con capacidad baja de almacenamiento de datos.

La primera vez que dos dispositivos intentan comunicarse, se utiliza un procedimiento de inicialización llamado emparejamieto para crear una clave de enlace común de una forma segura. El emparejamiento consiste en:

- Se genera un número aleatorio como clave de inicialización. El cual se utiliza una vez y luego se descarta.

- Mediante autenticación, el código de seguridad Bluetooth es comprobado para ver si es el mismo en los dos dispositivos a emparejar.

- Se genera un número aleatorio de 128 bits como clave de enlace común y se almacena temporalmente en los dispositivos emparejados. Mientras que esta clave de enlace esté almacenada en ambos dispositivos, no es necesario repetir el emparejamiento, en cuyo caso sólo se implementa el procedimiento normal para autenticación.

4.3 DESCRIPCIÓN GENERAL DE LA ARQUITECTURA

Una característica de la arquitectura de seguridad Bluetooth (figura 4.1) es que se evita en todo lo posible la intervención del usuario para

acceder a los servicios. La intervención del usuario se necesita únicamente para permitir a los dispositivos acceso limitado a los servicios o para establecer una relación de confianza con algún dispositivo, permitiendo acceso ilimitado a sus servicios.

El componente clave de la arquitectura de seguridad Bluetooth es el gestor de seguridad, el cual es responsable de realizar las siguientes tareas:

- Almacenar la información relacionada con la seguridad de los servicios.
- Almacenar la información relacionada con la seguridad de los dispositivos.
- Responder a las solicitudes de acceso de la implementación del protocolo o de la aplicación.
- Forzar la autenticación y/o cifrado antes de conectar con la aplicación.
- Iniciar o procesar los datos de entrada procedentes de una entidad externa de control de seguridad (ESCE, External Security Control Entity), es decir, el usuario del dispositivo, para establecer relaciones de confianza de nivel de dispositivo.

Iniciar el emparejamiento y solicitar la introducción de un PIN por parte del usuario. La introducción de un PIN también puede ser realizada por una aplicación.

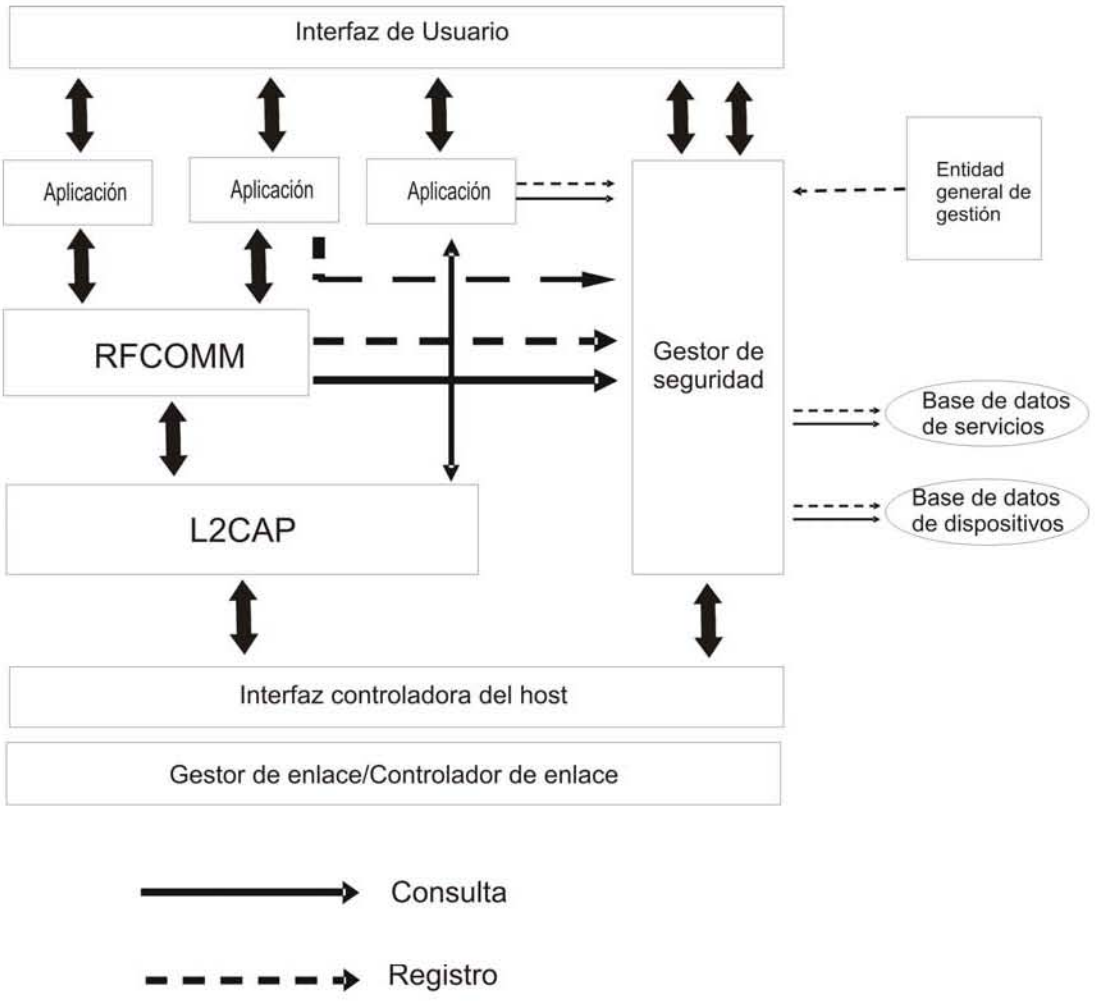

Figura 4.1 Arquitectura de seguridad Bluetooth Fuente: J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed**.** Mc Graw Hill, 2002.

4.4 NIVEL DE SEGURIDAD DE LOS SERVICIOS

Como se describe en la especificación Bluetooth, el nivel de seguridad de un servicio está definido por tres atributos:

- Necesidad de autorización. El acceso está garantizado automáticamente sólo a los dispositivos de confianza (es decir, aquellos dispositivos marcados como tales en la base de datos de dispositivos), o a dispositivos no de confianza después de un procedimiento de autorización. La autorización requiere siempre autenticación para verificar que el dispositivo remoto es el correcto.

- Necesidad de autenticación. Antes de conectarse a una aplicación, el dispositivo remoto debe ser autenticado.

- Necesidad de cifrado. El enlace debe cambiarse al modo cifrado antes de que sea permitido el acceso al servicio.

Esta información de los atributos está almacenada en la base de datos de servicios del gestor de seguridad. Si no ha tenido lugar ningún proceso de registro, se utiliza un nivel de seguridad predeterminado. Para una conexión entrante, el valor predeterminado es necesidad de autorización y autenticación. Para una conexión saliente el valor predeterminado es necesidad de autenticación.

4.5 ESTABLECIMIENTO DE LA CONEXIÓN

Para cumplir con los diferentes requisitos de disponibilidad de los servicios sin la intervención del usuario, la autenticación debe ser realizada después de determinar el nivel de seguridad del servicio requerido. Así, la autenticación no puede ser realizada cuando se establece el enlace asíncrono sin conexión (ACL).

La autenticación se realiza cuando se envía una solicitud de conexión a un servicio (figura 4.2).
La secuencia de sucesos que tiene lugar para acceder a un dispositivo de confianza es la siguiente:

- La solicitud de conexión pasa a través de L2CAP.
- L2CAP solicita acceso al gestor de seguridad.
- El gestor de seguridad realiza una consulta en la base de datos de servicios.
- El gestor de seguridad realiza una consulta en la base de datos de dispositivos.
- Si es necesario, el gestor de seguridad obliga ala autenticación y cifrado.
- El gestor de seguridad concede el acceso.
- L2CAP continúa con el establecimiento de la conexión.

La autenticación puede realizarse en ambas direcciones, permitiendo al cliente autenticar el servidor o el servidor autenticar al cliente.

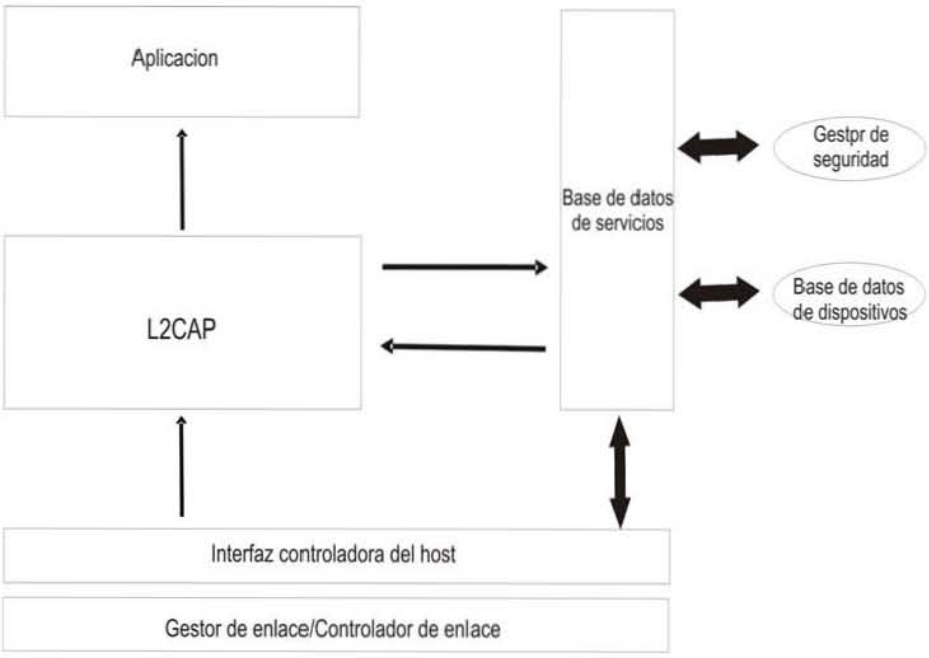

Figura 4.2 flujo de información para acceder a un dispositivo de confianza Fuente: J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed***.*** Mc Graw Hill, 2002, pág 275.

4.6 AUTENTIFICACIÓN EN EL ESTABLECIMIENTO DE ENLACE EN BANDA BASE

No está dirigida al Modo de seguridad 3, es decir, el modo con seguridad impuesta en el nivel de enlace, la arquitectura de seguridad Bluetooth puede soportar este modo también. El gestor de seguridad puede ordenar al gestor de enlace que fuerce a que se realice la autenticación antes de aceptar una conexión de banda base; utilizando la interfaz HCI (Host Controller .Interface, interfaz controladora del host). Sin embargo, antes de pasar del Modo 2 al Modo 3, deben tomarse medidas que impidan que los dispositivos no

de confianza puedan obtener un acceso no deseado. Con este fin, el gestor de seguridad borra todas las claves de enlace de los dispositivos no de confianza que estén almacenadas en el módulo de radio. Para esto, el gestor de seguridad puede utilizar la interfaz HCI.

4.7 GESTIÓN DE LA PILA DE PROTOCOLOS

Para las conexiones entrantes, el procedimiento de control de acceso está resumido (figura 4.3). El control de acceso es requerido en L2CAP y, en algunos casos, también en los protocolos de multiplexación superiores (por ejemplo, RFCOMM).

Cuando se recibe una solicitud de conexión, la entidad de protocolo consulta al gestor de seguridad, proporcionándole cualquier información de multiplexación que haya recibido junto con la solicitud de conexión. El gestor de seguridad determina si se concede o no el acceso y, entonces, responde a la entidad de protocolo. Si se concede el acceso, el procedimiento de establecimiento de la conexión continúa; si el acceso es denegado, se finaliza la conexión. Si no se realiza control de acceso en un nivel de protocolo, no tiene lugar ninguna interacción con el gestor de seguridad u otras entidades.

El gestor de seguridad almacena información sobre las autenticaciones existentes. Esto evita que se tengan que realizar procedimientos de autenticación múltiples! en el nivel LMP (es decir, sobre el aire) dentro de la misma sesión. Así, RFCOMM; hará una comprobación de política de seguridad con el gestor de seguridad; esto requiere una llamada de función adicional, pero no

necesariamente una autenticación adicional. Para las conexiones salientes, también puede ser necesaria una comprobación de seguridad para conseguir la autenticación mutua, en cuyo caso se lleva a cabo un procedimiento similar.

La manera más eficiente de enviar solicitudes al gestor de seguridad es que las envíen las aplicaciones directamente. Si esto no es posible, como en el caso de aplicaciones heredadas, las consultas al gestor de seguridad pueden ser enviadas por cualquier protocolo de multiplexación (Figura 4.4).

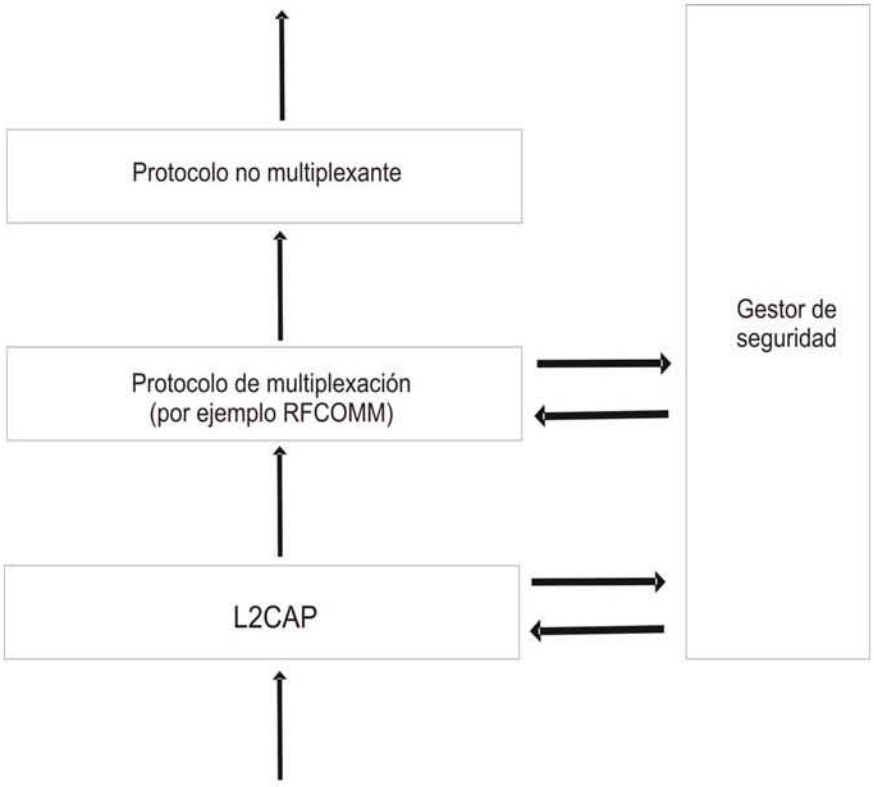

Figura 4.3 Comportamiento de los protocolos para las conexiones entrantes. Fuente: J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed**.** Mc Graw Hill, 2002, pág 277.

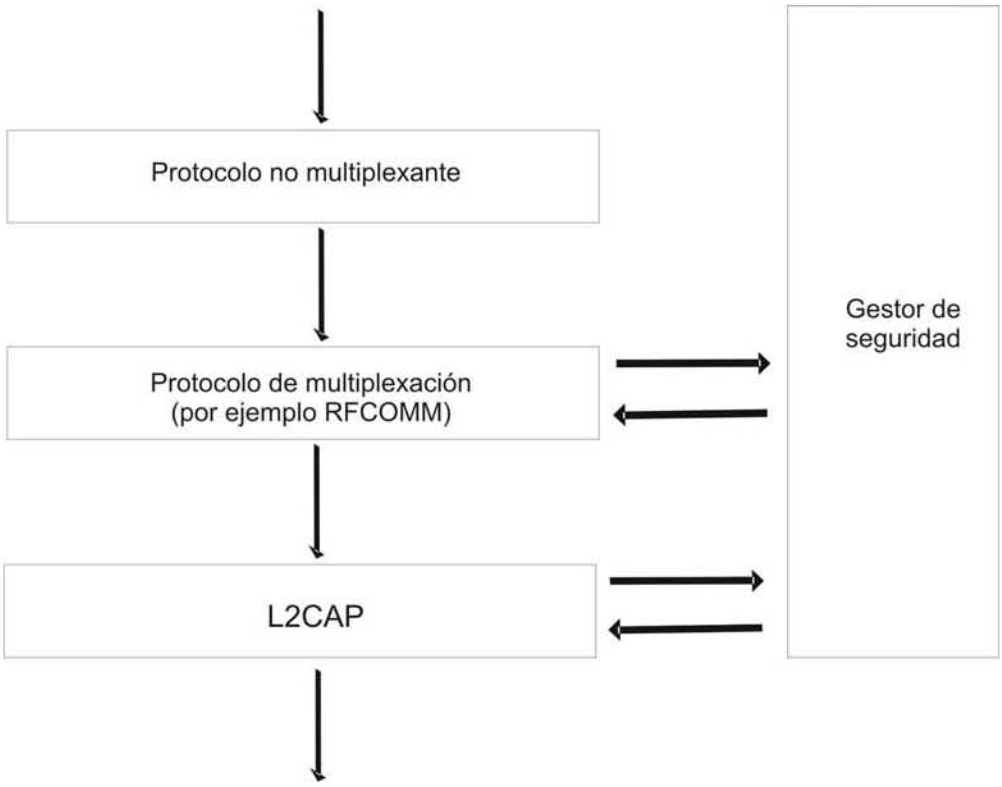

Figura 4.4. Comportamiento de los protocolos durante las conexiones salientes. Fuente: J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed**.** Mc Graw Hill, 2002, pág 277.

Como ya se ha indicado, el gestor de seguridad mantiene la información de seguridad relativa a los servicios en bases de datos de seguridad. Las aplicaciones deben registrarse ante el gestor de seguridad para poder ser accesibles (figura 4.5).

Las aplicaciones o sus delegados de seguridad deben proporcionar información sobre su nivel de seguridad sobre multiplexación al gestor de seguridad. Esta información es similar ala información que está registrada para el descubrimiento de servicios. El gestor de seguridad necesita esta información para tomar la decisión de conceder/denegar

una solicitud de acceso enviada por una entidad de protocolo, ya que esta entidad puede no ser siempre consciente de la aplicación final.
Las implementación de los protocolos de multiplexación que realizan consultas al registro del gestor de seguridad registran también cuál es la política para acceder a la información desde los niveles inferiores. Ambos registros pueden ser realizados también por la entidad responsable de establecer la ruta en la pila de protocolos Bluetooth. Qué entidad sea la que inicie el procedimiento de registro depende de la implementación.

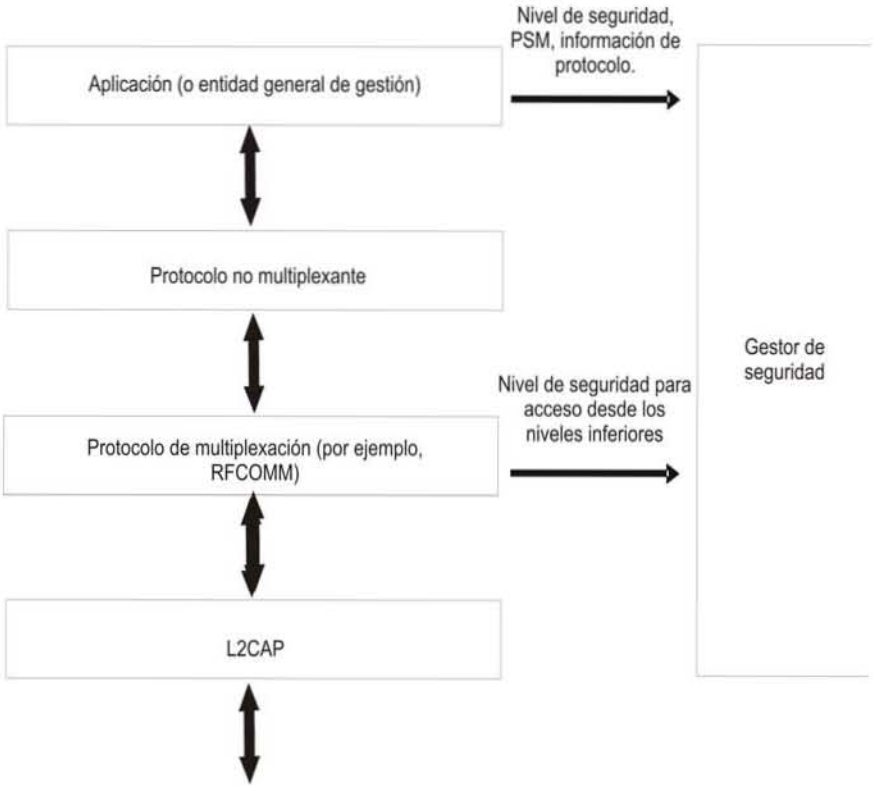

Figura 4.5 proceso de registro Fuente: J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª Edición Ed*.* Mc Graw Hill, 2002, pág 278.

4.8 INTERFAZ CON UNA ENTIDAD EXTERNA DE CONTROL DE SEGURIDAD

La arquitectura de seguridad Bluetooth incluye una interacción con el usuario para propósitos de autorización. Esto incluye el permiso de acceso a los servicios y el e! establecimiento de una relación de confianza con un dispositivo remoto. El gestor de
seguridad invoca a la entidad externa de control de seguridad (por ejemplo, la interfaz de usuario); los parámetros de entrada son la información enviada con la solicitud y los parámetros de salida contienen la respuesta.

Si el gestor de seguridad solicita un PIN, puede utilizarse una llamada a la entidad externa de control de seguridad. La introducción del PIN también puede ser solicitada directamente desde el gestor de enlace. El gestor de seguridad solicita entonces la autenticación y, si no hay disponible ningún enlace válido, el gestor de enlace lleva a cabo las acciones necesarias.

4.9 PROCEDIMIENTOS DE REGISTRO

Como ya hemos dicho, las aplicaciones deben registrarse ante el gestor de seguridad para poder ser accesibles. Algunos de los parámetros utilizados para registrar la aplicación y el protocolo de multiplexación son:

- ✓ Nombre coloquial de la aplicación, para las consultas del usuario.
- ✓ Nivel de seguridad.
- ✓ Multiplexor de protocolos/servicios (PSM), que es un valor utilizado en el nivel L2CAP.
- ✓ Identificación del protocolo.
- ✓ Identificación del canal.

El registro puede ser realizado por la entidad responsable de establecer la ruta en la pila de protocolos Bluetooth. Qué entidad realice el registro depende de la implementación. Si no se produce ningún registro, se aplican las opciones de configuración predeterminadas.

4.10 INTERFAZ CON HCI / GESTOR DE ENLACE

Según la especificación Bluetooth, HCI proporciona una interfaz de comandos para el controlador de banda base y el gestor de enlace, así como acceso a los registros de control y de estado del hardware. Esta interfaz proporciona un método uniforme para acceder a las capacidades de la banda base Bluetooth. Entre otras cosas, el gestor de seguridad puede ordenar al gestor de enlace, utilizando la interfaz HCI, que fuerce a que se realice una autenticación antes de aceptar una conexión de banda base.

- **SOLICITUD DE AUTENTICACIÓN**

El comando HCI_Authentication_Requested se utiliza para solicitar la autenticación de un dispositivo remoto. Como respuesta, se devuelve un suceso Authentication Complete.

- **CONTROL DE CIFRADO**

Para el control del cifrado, se utiliza el comando HCI_Set_Connection_Encryption. Como respuesta, se devuelve un suceso Encryption Change, que activa y desactiva el cifrado de nivel de enlace.

- **SOLICITUD DE NOMBRE AL DISPOSITIVO REMOTO**

Para la solicitud de nombre a un dispositivo remoto, se utiliza el comando HCI_Remote_Name_Request, con el fin de obtener el nombre descriptivo del otro dispositivo Bluetooth. El nombre descriptivo permite al usuario distinguir un dispositivo Bluetooth de otro. El parámetro BD_ADDR del comando se utiliza para identificar el dispositivo del que se desea obtener el nombre descriptivo. En respuesta al comando de solicitud de nombre remoto, se devuelve Remote_Name_Request Complete.

4.11 ESTABLECIMIENTO DE LA POLÍTICA DE CIFRADO DE NIVEL DE ENLACE

La política general de cifrado en el nivel de enlace puede ser establecida con el comando HCI- Write_EncryptioJi_Mode, al que se

responde con el suceso Command Complete. El parámetro Encryption Mode controla si la radio Bluetooth requerirá cifrado en el nivel de enlace para cada conexión con otras radios Bluetooth.

4.12 ESTABLECIMIENTO DE LA POLÍTICA DE AUTENTICACIÓN EN EL NIVEL DE ENLACE

La política general de autenticación en el nivel de enlace puede establecerse con el comando HCI- Write_Authentication_Enable. El parámetro Authentication_Enable controla si la radio Bluetooth requerirá autenticación en el nivel de enlace para cada conexión con otras radios Bluetooth. Durante el establecimiento de la conexión, solamente aquellos dispositivos que tengan el parámetro Authentication_Enable habilitado intentará autenticar el otro dispositivo. El comando Read_Authentication_Enable permite leer el valor del parámetro Authentication_Enable. Cuando se termina de ejecutar el comando Read_Authentication_Enable, se generará un suceso Command Complete.

CONCLUSIÓN

Mediante esta tesis abordo los temas de la creciente evolución tecnológica inalámbrica, transmisión de alta velocidad para aplicaciones multimedia y acceso a Internet. Los mercados para todas estas características antes mencionadas ya existen y crecerán a un ritmo acelerado en los próximos años.

Gracias a su pequeño tamaño, gran funcionalidad, flexibilidad y su bajo costo, la tecnología Bluetooth es y seguirá siendo incorporada en múltiples dispositivos de mano y aparatos electrónicos, ofreciendo capacidades de control y de acceso a la información de una manera simple y elegante. La nueva generación de sistemas de telefonía celular, empleando la especificación Bluetooth se interconectan donde quiera que estén o donde vayan. La tecnología inalámbrica Bluetooth extiende y seguirá evolucionando el alcance de los sistemas celulares bastante más allá de las fronteras actuales.

Por tales motivos propongo el considerar esta tecnología inalámbrica ya que ofrece ventajas competitivas en el campo informático y de las telecomunicaciones, consta de una gran versatilidad y eficacia, para poderse emplear donde el usuario crea mas conveniente.

BIBLIOGRAFIA

J. MULLER, Nathan, ***Tecnología Bluetooth,*** 2ª edición Editorial Mc Graw Hill, España, 2002, p.p. 386.

OTRAS FUENTES

http://www.zonabluetooth.com

http://www.tiramillas.net

www.bluetooth.com

www.bluetooth.org

http://www.e-global.es

http://www.umtsforum.net

http://www.terra.es

http://www.palowireless.com

http://www.microsoft.com

http://www.datex-ohmeda.es

http://www.monografias.com

http://www.wmlclub.com/cgi

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.bluetooth.com&e=articulos

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.bluetooth.net&e=articulos

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.atmel.com/bluetooth/&e=articulos.

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.countersys.com/tech/bluetooth.html&e=articulos

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.nokia.com/phones/bluetooth/index.html&e=articulos

http://www.wmlclub.com/cgi-bin/estadis/check2.pl?d=http://www.intel.com/mobile/bluetooth/index.htm&e=articulos