UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA.

ING. ELECTRÓNICA Y TELECOMUNICACIONES.

"BLUETOOTH"

MONOGRAFÍA

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES.

PRESENTA:

GARCÍA VARGAS ALEJANDRO.

ASESOR:

ING. ARUMIR RIVAS MARIANO.

ÍNDICE.

JUSTIFICACIÒN.

La necesidad de comunicación ha estado presente en el pensamiento del hombre desde que llegó al mundo, arcaicos medios de comunicación y transferencia de datos han sido necesarios para la sobre vivencia, estos medios fueron avanzando hasta la creación del lenguaje. Pero el ser humano es cambiante, buscador nato de nuevas formas que hagan su vida más cómoda, es por ello que a través del tiempo ha evolucionado la manera de comunicarse como lo ha hecho con las Telecomunicaciones usando dispositivos electrónicos como teléfonos, computadoras, fax, entre muchos otros.

La tecnología Bluetooth es una nueva evolución que el hombre ha hecho para mejorar la forma de transmisión de datos y así hacer más fácil, cómoda, confiable, segura, y rápida la comunicación entre las personas. Ya que Bluetooth es una nueva tecnología hoy en día no se conoce mucho acerca de ella y por tal motivo es objeto de estudio y de recopilación de información.

Esta monografía esta enfocada para enriquecer el acervo cultural de la Biblioteca Central de la Universidad Autónoma del Estado de Hidalgo porque constituye un documento de consulta para estudiantes y maestros de Telecomunicaciones venideros ya que es una fuente de información teórica acerca de que es, como trabaja y sus aplicaciones de la tecnología Bluetooth.

INTRODUCCIÒN.

Bluetooth es una tecnología utilizada para conectividad inalámbrica de corto alcance entre dispositivos tales como PDAs (Personal Digital Assistance), teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, módems, proyectores, impresoras, etc. El principal mercado es la transferencia de datos y voz entre dispositivos y computadoras personales. El enfoque de Bluetooth es similar a la tecnología de infrarrojo conocida como IrDA (Infrared Data Association). Sin embargo, Bluetooth, es una tecnología de radiofrecuencia (RF) que utiliza la banda de espectro disperso de 2.4 GHz. Muchas veces también se le confunde con el estándar IEEE 802.11, otra tecnología de RF de corto alcance. IEEE 802.11 ofrece más caudal eficaz pero necesita más potencia de transmisión y ofrece menos opciones de conectividad que Bluetooth para el caso de aplicaciones de voz.

Bluetooth intenta proveer significantes ventajas sobre otras tecnologías inalámbricas similares tales como IrDA y HomeRF, claros competidores en conexiones PC a periféricos. IrDA es una tecnología muy popular para conectar periféricos, pero es limitada severamente a conexiones de cortas distancias en rangos de un metro por la línea de vista requerida para la comunicación. Debido a que Bluetooth funciona con RF no está sujeto a tales limitaciones. Las distancia de conexión en Bluetooth puede ser de hasta 10 metros o más dependiendo del incremento de la potencia del transmisor, pero los dispositivos no necesitan estar en línea de vista ya que las señales de RF pueden atravesar paredes y otros objetos no metálicos sin ningún problema.

Bluetooth puede ser usado para aplicaciones en redes residenciales o en pequeñas oficinas, ambientes que son conocidos como WPANs (Wireless Personal Area Network). Una de las ventajas de las tecnologías inalámbricas es que evitan el problema de alambrar las paredes de las casas u oficinas.

OBJETIVOS.

Objetivo General.

Proveer de una visión general de la tecnología actual y definir su tendencia en el futuro eliminando cables y conectores entre equipos.

Objetivos Específicos.

- Ofrecer la posibilidad de crear pequeñas redes inalámbricas.
- Facilitar la sincronización de datos entre nuestros equipos personales en la tecnología Bluetooth.
- Implementar los servicios de movilidad y despliegue inalámbrico que permiten soluciones integradas e integrales en toda una empresa en menos tiempo y con menos riesgos.
- Conciliar el nuevo desarrollo de movilidad y las continuas actualizaciones en la infraestructura de la empresa.
- Desarrollar y estudiar las implicaciones del acelerado cambio de la tecnología analógica a la digital en los sistemas de comunicaciones.
- Explicar la gran variedad de aplicaciones que se pueden implementar utilizando las nuevas tecnologías y servicios de comunicaciones.
- Evaluar los diferentes estándares existentes de la tecnología inalámbrica con el fin de definir las diferencias entre ellos y como cada uno de ellos pueden interactuar en la red.

CAPÍTULO 1:

REDES

INALÁMBRICAS.

1.1 TECNOLOGÍA INALÁMBRICA.

La tecnología inalámbrica es aquel sistema capaz de conectar equipos terminales a la red de datos sin necesidad de utilizar cables de comunicación para ello. Es una tecnología en la cual los medios de comunicación entre sus componentes son ondas electromagnéticas.

Actualmente el término se refiere a comunicación sin cables, usando frecuencias de radio u ondas infrarrojas. Entre los usos más comunes se incluyen a IrDA y las redes inalámbricas de computadoras. Ondas de radio de bajo poder, como los que se emplean para transmitir información entre dispositivos, normalmente no tienen regulación, en cambio, transmisiones de alto poder requieren un permiso del estado para poder trasmitir en una frecuencia específica.

1.2 TIPOS DE REDES INALÁMBRICAS.

Algunas de las técnicas utilizadas en las redes inalámbricas son: infrarrojos, Bluetooth, Wi-Fi y WiMAX.

1.2.1 Infrarrojo.

Las redes por infrarrojos permiten la comunicación entre dos nodos con velocidades hasta 4 Mbps, usando una serie de leds infrarrojos para ello.

La redes IR (Infrarrojo) permiten conectar dos dispositivos con puertos IR incorporados y ubicados en el mismo espacio o ambiente. Simplemente se alinean los puertos IR de cada dispositivo y se transmiten o envían los datos.

Las ideas que debemos tener presentes a la hora de pensar en infrarrojos deben ser: visión directa, distancias relativamente cortas, esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos.

1.2.2 Bluetooth.

Bluetooth es una frecuencia de radio de disponibilidad universal que conecta entre sí los dispositivos habilitados para Bluetooth situados a una distancia de hasta 10 metros. Permite conectar un ordenador portátil o un dispositivo de bolsillo con otros ordenadores portátiles, teléfonos móviles, cámaras, impresoras, teclados, altavoces, etc.

Permite conectar de forma rápida con velocidades de hasta 780 Kbps. y sencilla los dispositivos habilitados para Bluetooth entre sí y de este modo crear una red de área personal (PAN) en la que es posible combinar todas las herramientas de trabajo principales con todas las prestaciones de la oficina. El uso de una red de igual a igual Bluetooth permite intercambiar archivos en reuniones improvisadas con suma facilidad y ahorrar tiempo imprimiendo documentos sin necesidad de conectarse a una red fija o inalámbrica. Con Bluetooth, se puede hacer actividades de inmediato como imprimir un informe desde el escritorio mediante cualquier impresora habilitada para Bluetooth dentro del radio, sin cables, sin problemas y sin moverse siquiera.

1.2.3 Wi-Fi

Wi-Fi o red de área local inalámbrica (WLAN) es una red de tamaño medio que utiliza la frecuencia de radio 802.11a, 802.11b o 802.11g en lugar de cables y permite realizar diversas conexiones inalámbricas a Internet con velocidades entre 11 Mbps. y 54 Mbps. Si sabe dónde se encuentra una red Wi-Fi o WLAN, se puede navegar por Internet, utilizar el correo electrónico y acceder a la red privada de una empresa.

Donde haya una red Wi-Fi, existe un portal de información y comunicación. La incorporación de una red WLAN a la oficina proporciona una mayor libertad y favorece la versatilidad del entorno de trabajo tradicional. Ahora bien, estas posibilidades no se limitan a la oficina, y cada vez aparecen más redes WLAN en lugares como restaurantes, hoteles y aeropuertos, lo que permite a los usuarios acceder a la información que necesitan. Acceda a la red de la empresa y obtenga las respuestas que necesite, en el momento preciso. Wi-Fi pone a su disposición un acceso a Internet sin igual.

1.2.3 WiMAX

WiMAX (del inglés *Worldwide Interoperability for Microwave Access*, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (802.MAN) proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, posee un ancho de banda entre 2-11 GHz.

CAPÍTULO 2:

LA TECNOLOGÍA BLUETOOTH.

2.1 ANTECEDENTES HISTÓRICOS

El origen del nombre de la tecnología Bluetooth proviene de un Vikingo de origen Danés Harald Blatand (Bluetooth) quien en el siglo décimo unificó Dinamarca y Noruega. El nombre fue adoptado por Ericsson, quien espera que Bluetooth unifique las telecomunicaciones y la industria del cómputo.

La versión 1.0 de la especificación Bluetooth fue liberada en 1999, pero el desarrollo de esta tecnología empezó realmente 5 años atrás, en 1994, cuando la compañía Ericsson empezó a estudiar alternativas para comunicar los teléfonos celulares con otros dispositivos. El estudio demostró que el uso de enlaces de radio sería el más adecuado, ya que no es directivo y no necesita línea de vista; eran tan obvias estas ventajas con respecto a los enlaces vía infrarrojo que son utilizados para conectar dispositivos y teléfonos celulares. Existían muchos requerimientos para el estudio, los cuales incluían la manipulación tanto de voz como de datos, de tal manera se podrían conectar teléfonos a dispositivos de cómputo. Así es como nace la especificación de la tecnología inalámbrica conocida como Bluetooth. [1]

2.2 BLUETOOTH SIG (Special Interest Group)

El Bluetooth SIG es un grupo de compañías trabajando juntas para promover y definir la especificación Bluetooth. Bluetooth SIG fue fundado en febrero de 1998 por las siguientes compañías: Ericsson, Intel, IBM, Toshiba y Nokia. En mayo de 1998, se anuncia públicamente el Bluetooh SIG y se invita a otras compañías para que se unan a éste. Fué en julio de 1999 cuando el SIG publica la versión 1.0 de la especificación de Bluetooth. En diciembre de 1999, se unen otras compañías tales como Microsoft, Lucent, 3Com y Motorola.

2.3 DEFINIÓN DE BLUETOOTH.

La tecnología Bluetooth tiene muchas definiciones desde muchos puntos de vista.

La idea primordial es proveer de una conexión inalámbrica y fácil de usar, de manera que pueda ser usada ésta conexión para diferentes funcionalidades.

Bluetooth es el nombre de una nueva tecnología que está ahora comercialmente disponible. Promete cambiar significativamente la manera en que usamos las máquinas.

Es un estándar empleado en enlaces de radio de corto alcance. La tecnología empleada permite a los usuarios conexiones instantáneas de voz y datos entre varios dispositivos en tiempo real. El modo de transmisión empleado, asegura protección contra interferencias y seguridad en el envío de datos. [2]

Bluetooth es un estándar desarrollado por un grupo de fabricantes electrónicos que permite que cualquier tipo de equipo electrónico desde computadoras y teléfonos celulares, hasta teclados y audífonos establezca sus propias conexiones, sin cables u otra acción directa de un usuario, como se muestra en la Fig. 2.1:

Fig.2.1: Representación grafica de la Tecnología Bluetooth.

CAPÍTULO 3:

FUNCIONAMIENTO DE BLUETOOTH.

3.1 BANDA DE FRECUENCIA LIBRE.

Los dispositivos Bluetooth están compuestos por dos partes principales. Un dispositivo de radio, encargado de modular y transmitir la señal, y un controlador digital.

El radio Bluetooth es un pequeño microchip que opera en una banda de frecuencia disponible mundialmente. Pueden realizarse comunicaciones punto a punto y punto multipunto.

Para poder operar en todo el mundo es necesaria una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar del planeta donde nos encontremos. Sólo la banda ISM (médico-científica internacional) de 2,45 GHz cumple con éste requisito, con rangos que van de los 2.4 MHz a los 2.5 MHz, y sólo con algunas restricciones en países como Francia, España y Japón, como se muestra en la Fig.3.1:

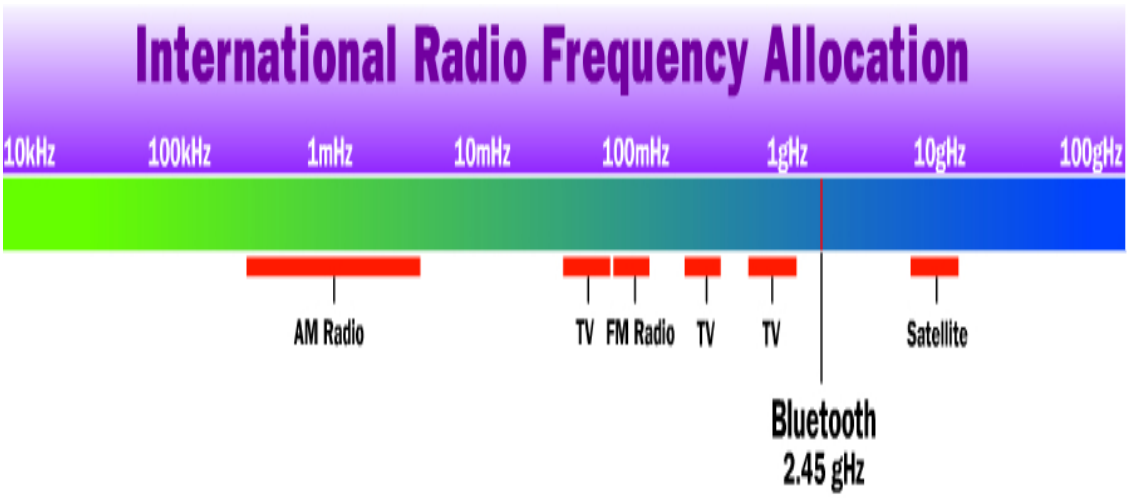

Fig.3.1 Ubicación de la frecuencia utilizada por Bluetooth.

En México el intervalo de frecuencias va de 2.450 MHz a 2.485 MHz. En los Estados Unidos y Europa, el rango de frecuencias es desde 2.4 MHz. hasta 2.483 MHz, con 79 canales de frecuencias de radio de 1MHz. En la práctica, el rango es de 2.402 MHz hasta 2.480 MHz. En Japón el rango de frecuencias va desde 2.472 MHz. hasta 2.497 MHz, con 23 canales de frecuencia de radio de 1Mhz.

3.2 FORMA DE TRANSMISIÓN.

Bluetooth opera en la banda 2.4 GHz bajo la tecnología de radio conocida como espectro disperso. La banda de operación está dividida en canales de 1 MHz, a 1 mega símbolo por segundo puede obtenerse al ancho de banda máximo por canal.

Con el esquema de modulación empleado, GFSK (Gaussian Frequency Shift Keying), esto equivale a 1 Mbps. Utilizando GFSK, un 1 binario representa una desviación positiva de la portadora nominal de la frecuencia, mientras que un 0 representa una desviación negativa. Después de cada paquete, ambos dispositivos re-sintonizan su radio transmisor a una frecuencia diferente, saltando de un canal a otro canal de radio; ésta técnica se le conoce como espectro disperso con salto en frecuencia (FHSS, Frequency Hopping Spread Spectrum).

De ésta manera, los dispositivos Bluetooth utilizan toda la banda de 2.4 GHz y si una transmisión se interfiere sobre un canal, una retransmisión siempre ocurrirá sobre un canal diferente con la esperanza de que éste canal sea libre.

Cada ranura de tiempo tiene una duración de 625 microsegundos y generalmente los dispositivos saltan una vez por paquete, o sea, saltan cada ranura, cada 3 ranuras ó cada 5 ranuras. Como Bluetooth fue diseñado para aplicaciones móviles de poca potencia, la potencia del radio transmisor debe ser minimizada.

Tres diferentes clases de niveles de potencias están definidas, las cuales proveen rangos de operación de aproximadamente 10, 20 y 100 metros: El más bajo nivel de potencia cubre 10 metros, el más alto nivel logra cubrir distancias de hasta 100 metros.

Aunado a las distancias cortas de conexión de Bluetooth en materia de ancho de banda soporta hasta 780 Kbps, los cuales pueden ser utilizados para transferir unidireccionalmente 721 Kbps y 57.6 Kbps en la dirección de retorno o hasta 432.6 Kbps de manera simétrica en ambas direcciones. [3]

3.2.1 Definición de Canal.

Como se ha visto, Bluetooth utiliza un sistema transmisión de espectro disperso con salto de frecuencia (FHSS, Frequency Hopping Spread Spectrum), en el que el canal queda dividido en intervalos de 625 μs, llamados slots, donde cada salto de frecuencia es ocupado por un slot. Esto da lugar a una frecuencia de salto de 1600 veces por segundo, en la que un paquete de datos ocupa un slot para la emisión y otro para la recepción y pueden ser usados alternativamente.

Dos o más unidades Bluetooth pueden compartir el mismo canal formando una piconet , donde una unidad actúa como maestra, controlando el tráfico de datos en la piconet que se genera entre las demás unidades, donde éstas actúan como esclavas, enviando y recibiendo señales hacia el maestro.

El salto de frecuencia del canal está determinado por la secuencia de la señal, es decir, el orden en que llegan los saltos y por la fase de ésta secuencia. En Bluetooth, la secuencia queda fijada por la identidad de la unidad maestra de la piconet (un código único para cada equipo), y por su frecuencia de reloj.

Como los dispositivos Bluetooth operan en 2 modos: como maestro y como esclavo. Si el maestro asigna la secuencia de salto de frecuencia. Los esclavos sincronizan al dispositivo maestro en tiempo y frecuencia seguido de la secuencia de salto del dispositivo maestro como se muestra en la Fig. 3.2:

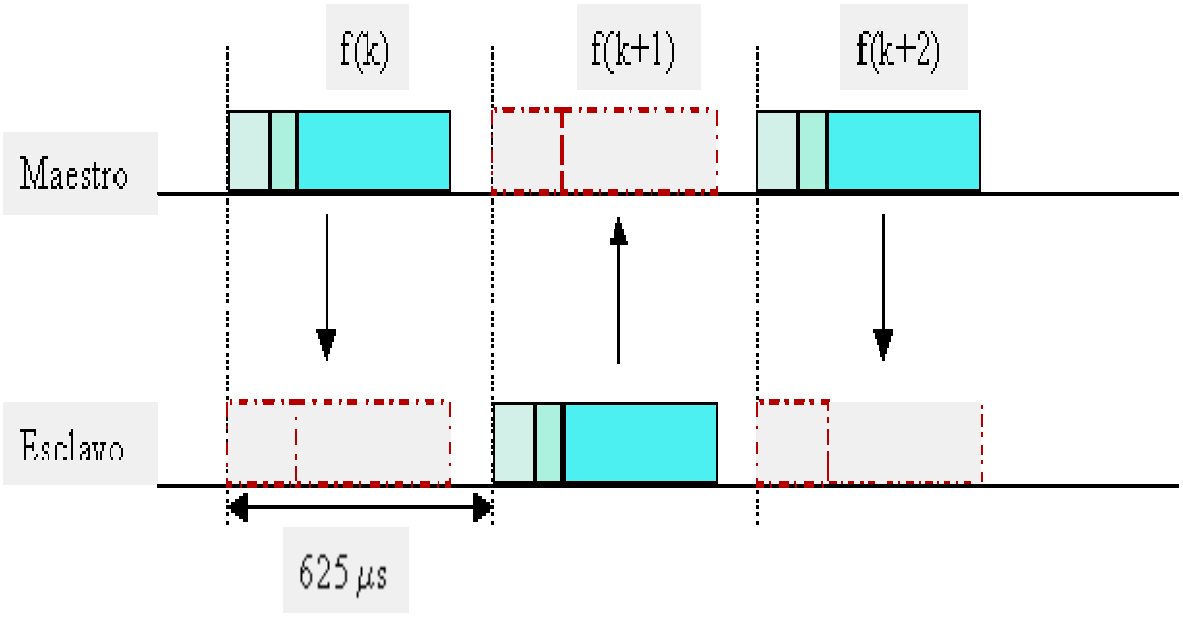

Fig.3.2: Canal Bluetooth.

3.2.2 Definición de Paquete.

La información que se intercambia entre dos unidades Bluetooth se realiza mediante un conjunto de slots que forman un paquete de datos. Cada paquete comienza con un código de acceso de 72 bits, que se deriva de la identidad maestra, seguido de un paquete de datos de cabecera de 54 bits. El cual contiene importante información de control, como tres bits de acceso de dirección, tipo de paquete, bits de control de flujo, bits para la retransmisión automática de la pregunta, y chequeo de errores de campos de cabeza. Finalmente, el paquete que contiene la información, que puede seguir al de cabeza, tiene una longitud de 0 a 2745 bits. En cualquier caso, cada paquete que se intercambia en el canal está precedido por el código de acceso, como se muestra en la Fig. 3.3:

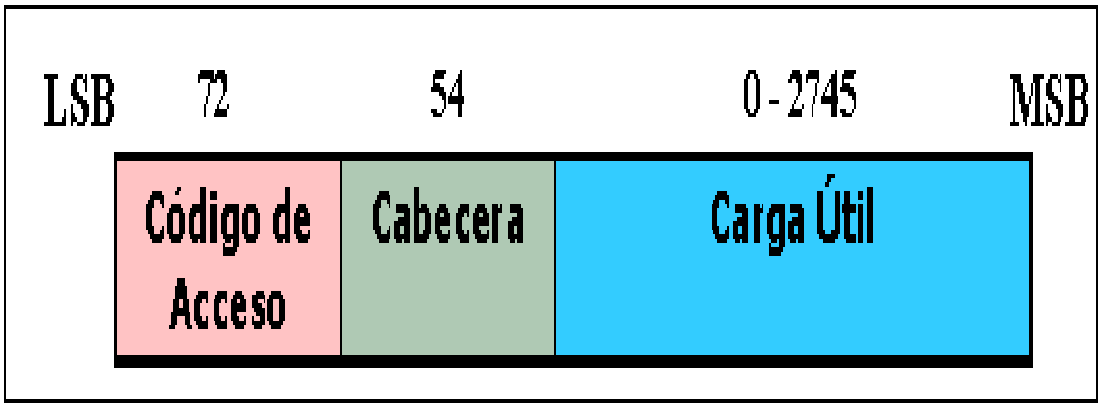

Fig.3.3: Paquete Bluetooth.

Los receptores de la piconet comparan las señales que reciben con el código de acceso, si éstas no coinciden, el paquete recibido no es considerado como válido en el canal y el resto de su contenido es ignorado. [4]

3.3 TIPOS DE ENLACE.

En la tecnología Bluetooth se han definido dos tipos de enlace que permitan soportar incluso aplicaciones multimedia:

- Enlace de sincronización de conexión orientada (SCO)
- Enlace asíncrono de baja conexión (ACL)

3.3.1 Enlace de Sincronización de Conexión Orientada (SCO).

Los enlaces SCO soportan conexiones asimétricas, punto a punto, usadas normalmente en conexiones de voz, estos enlaces están definidos en el canal, reservándose dos slots consecutivos (envío y retorno) en intervalos fijos. Para los enlaces SCO, existen tres tipos de slot simple, cada uno con una portadora a una velocidad de 64 kbit/s.

Al dispositivo esclavo siempre se le permitirá responder durante la ranura de tiempo inmediatamente seguido de una transmisión tipo SCO del maestro. Un dispositivo maestro puede soportar hasta tres enlaces SCO a uno o varios esclavos, pero un sólo esclavo puede soportar sólo enlaces SCO para diferentes dispositivos maestros. Los paquetes SCO nunca son retransmitidos.

3.3.2 Enlaces Asíncronos de Baja Conexión (ACL).

Los enlaces orientados a no-conexión (ACL, Asynchronous Connectionless) son típicamente empleados para transmisión de datos. Las transmisiones sobre estos enlaces son establecidas en base por ranura (en ranuras no reservadas para enlaces SCO). Para los enlaces ACL, se han definido el slot-1, slot-3, slot-5. Cualquiera de los datos pueden ser enviados protegidos o sin proteger con una máxima velocidad de envío de 721 kbit/s en una dirección y 57.6 kbit/s en la otra.

Los enlaces ACL soportan transferencias punto-multipunto de datos asíncronos como síncronos. Después de una transmisión ACL del maestro, sólo el dispositivo esclavo direccionado puede responder durante la siguiente ranura de tiempo o si el dispositivo no está direccionado, los paquetes son considerados como mensajes difundidos (broadcast). La mayoría de los enlaces ACL incluyen retransmisión de paquetes. [5]

3.4 ADMINISTRADOR DE ENLACES.

La máquina de estado de banda base es controlada por el administrador de enlaces. Este micro código provee el control del enlace basado en hardware para configuración, seguridad y control de enlaces. Sus capacidades incluyen autentificación y servicios de seguridad, monitoreo de calidad de servicio y control del estado de banda base. El administrador de enlaces se comunica con los demás utilizando el protocolo LMP (Link Management Protocol), el cual utiliza los servicios básicos de banda base. Los paquetes LMP, los cuales son enviados

sobre los enlaces ACL, son diferenciados de los paquetes L2CAP (Logical Link Control and Adaptation Protocol) por un bit en el encabezado del ACL. Ellos son siempre enviados como paquetes de una ranura y una prioridad alta que los paquetes L2CAP. Esto ayuda el aseguramiento de la integridad del enlace bajo una alta demanda de tráfico. [2]

3.5 INMUNIDAD A LAS INTERFERENCIAS.

Bluetooth opera en una banda de frecuencia que está sujeta a considerables interferencias, por lo que el sistema ha sido optimizado para evitar éstas interferencias. En este caso la técnica de salto de frecuencia es aplicada a una alta velocidad y una corta longitud de los paquetes (1600 saltos/segundo, para slots-simples).

Los paquetes de datos están protegidos por un esquema ARQ (repetición automática de consulta), en el cual los paquetes perdidos son automáticamente retransmitidos; aun así, con este sistema, si un paquete de datos no llegase a su destino, sólo una pequeña parte de la información se perdería.

La voz no se retransmite nunca, sin embargo, se utiliza un esquema de codificación muy robusto. El esquema, se basa en una modulación variable de declive delta (CSVD), que sigue la forma de la onda de audio y es muy resistente a los errores de bits. Los errores son percibidos como ruido de fondo, que se intensifica si los errores aumentan. [2]

3.6 RED INALÁMBRICA BLUETOOTH.

Los sistemas Bluetooth crean una red personal (PAN), o Piconet, que puede llenar una habitación puede comprender una distancia no mayor que entre un teléfono celular en la cintura y unos audiófonos en la cabeza. Una vez que una Piconet está establecida, los miembros saltan de frecuencias al azar uno a uno, de forma tal que estén en contacto unos con otros y evitando otras Piconet que puedan operar en la misma habitación.

Bajo la especificación actual, hasta 8 dispositivos Bluetooth pueden automáticamente configurarse para formar una Piconet, con uno de ellos designados como el maestro y siete como esclavos. La Piconet se distingue de otras redes similares por su secuencia de saltos de frecuencia. [2]

3.6.1 Piconet.

Si un equipo se encuentra dentro del radio de cobertura de otro, éstos pueden establecer conexión entre ellos. En principio sólo son necesarias un par de unidades con las mismas características de hardware para establecer un enlace. Dos o más unidades Bluetooth que comparten un mismo canal forman una piconet. Para regular el tráfico en el canal, una de las unidades participantes se convertirá en maestra, pero por definición, la unidad que establece la piconet asume éste papel y todos los demás serán esclavos.

Los participantes podrían intercambiar los papeles si una unidad esclava quisiera asumir el papel de maestra. Sin embargo sólo puede haber un maestro en la piconet al mismo tiempo.

Cada unidad de la piconet utiliza su identidad maestra y reloj nativo para seguir en el canal de salto. Cuando se establece la conexión, se añade un ajuste de reloj a la propia frecuencia de reloj nativa de la unidad esclava para poder sincronizarse con el reloj nativo del maestro. El reloj nativo mantiene siempre constante su frecuencia, sin embargo los ajustes producidos por las unidades esclavas para sincronizarse con el maestro, sólo son válidos mientras dura la conexión.

Como ya hemos comentado, las unidades maestras controlan el tráfico del canal, por lo que estas tienen la capacidad para reservar slots en los enlaces SCO. Para los enlaces ACL, se utiliza un esquema de sondeo. A una esclava sólo se le permite enviar un slot a un maestro cuando ésta se ha dirigido por su dirección MAC (medio de control de acceso) en el procedimiento de slot maestro-esclavo. Éste tipo de slot implica un sondeo por parte del esclavo, por lo que, en un tráfico normal de paquetes, es enviado a una urna del esclavo automáticamente. Si la información del esclavo no está disponible, el maestro puede utilizar un paquete de sondeo para sondear al esclavo explícitamente. Los paquetes de sondeo consisten únicamente en uno de acceso y otro de cabecera. Dicho esquema de sondeo central elimina las colisiones entre las transmisiones de los esclavos.

Aunque una Piconet no puede contener más de 8 dispositivos, su alcance puede extenderse adjuntando un esclavo a otra Piconet. Lo anterior significa que un esclavo puede servir a más de un maestro en Bluetooth. [2]

3.6.2 Comunicación INTER-PICONET.

En un conjunto de varias piconet, los cuales seleccionan diferentes saltos de frecuencia y están controladas por diferentes maestros, por lo que si un mismo canal de salto es compartido temporalmente por piconet independientes, los paquetes de datos podrán ser distinguidos por el código de acceso que les precede, que es único en cada piconet.

La sincronización de varias piconet no está permitida en la banda ISM. Sin embargo, las unidades pueden participar en diferentes piconet en base a un sistema TDM (división de tiempo múltiplexada). Esto es, una unidad participa secuencial mente en diferentes piconet, a condición de que ésta este sólo activa en una al mismo tiempo. Una unidad al incorporarse a una nueva piconet debe modificar el offset (ajuste interno) de su reloj para minimizar la deriva entre su reloj nativo y el del, por lo que gracias a éste sistema se puede participar en varias piconet realizando cada vez los ajustes correspondientes una vez conocidos los diferentes parámetros de la piconet.

Cuando una unidad abandona una piconet, la esclava informa el maestro actual que ésta no estará disponible por un determinado periodo, que será en el que estará activa en otra piconet. Durante su ausencia, el tráfico en la piconet entre el maestro y otros esclavos continúa igualmente.

De la misma manera que una esclava puede cambiar de una piconet a otra, una maestra también lo puede hacer, con la diferencia de que el tráfico de la piconet

se suspende hasta la vuelta de la unidad maestra. La maestra que entra en una nueva piconet, en principio, lo hace como esclava, a no ser que posteriormente ésta solicite actuar como maestra. [2]

3.6.3 Scatternet.

Los equipos que comparten un mismo canal sólo pueden utilizar una parte de su capacidad de este. Aunque los canales tienen un ancho de banda de un 1Mhz, cuantos más usuarios se incorporan a la piconet, disminuye la capacidad hasta unos 10 kbit/s más o menos. Teniendo en cuenta que el ancho de banda medio disponible es de unos 80 Mhz en Europa y USA (excepto en España y Francia), éste no puede ser utilizado eficazmente, cuando cada unidad ocupa una parte del mismo canal de salto de 1Mhz. Para poder solucionar éste problema se adoptó una solución de la que nace el concepto de scatternet.

Las unidades que se encuentran en el mismo radio de cobertura pueden establecer potencialmente comunicaciones entre ellas. Sin embargo, sólo aquellas unidades que realmente quieran intercambiar información comparten un mismo canal creando la piconet. Por tal motivo se permite que se creen varias piconet en áreas de cobertura superpuestas.

A un grupo de piconet se le llama scatternet. El rendimiento, en conjunto e individualmente de los usuarios de una scatternet es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1 Mhz, como se muestra en la Fig.3.4:

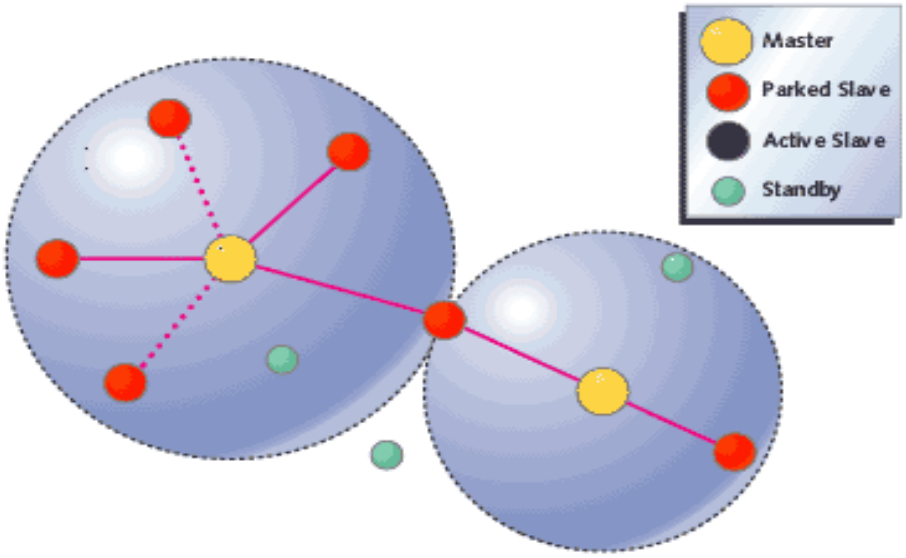

Fig.3.4: Ejemplo de Escatternet.

Además, estadísticamente se obtienen ganancias por multiplexación y rechazo de canales salto. Debido a que individualmente cada piconet tiene un salto de frecuencia diferente, diferentes piconet pueden usar simultáneamente diferentes canales de salto.

Hemos de tener en cuenta que cuantas más piconet se añaden a la scatternet el rendimiento del sistema FH (Salto de frecuencia) disminuye poco a poco, habiendo una reducción por termino medio del 10%. Sin embargo el rendimiento que finalmente se obtiene de múltiples piconet supera al de una simple piconet. [2]

3.7 ESTABLECIMIENTO DE UNA CONEXIÓN.

De un conjunto total de 79 (23) portadoras del salto, un subconjunto de 32(16) portadoras activas han sido definidas. El subconjunto, que es seleccionado pseudo-aleatóriamente, se define por una única identidad.

Acerca de la secuencia de activación de las portadoras, se establece que, cada una de ellas visitará cada salto de portadora una sola vez, con una longitud de la secuencia de 32 (16) saltos. En cada uno de los 2.048 (1.028) saltos, las unidades que se encuentran en modo *standby* (en espera) mueven sus saltos de portadora siguiendo la secuencia de las unidades activas. El reloj de la unidad activa siempre determina la secuencia de activación.

Durante la recepción de los intervalos, en los últimos 18 slots o 11,25 ms, las unidades escuchan una simple portadora de salto de activación y correlacionan las señales entrantes con el código de acceso derivado de su propia identidad. Si los triggers son correlativos, es decir, si la mayoría de los bits recibidos coinciden con el código de acceso, la unidad se auto-activa e invoca un procedimiento de ajuste de conexión. Sin embargo si estas señales no coinciden, la unidad vuelve al estado de reposo hasta el siguiente evento activo.

Para establecer la piconet, la unidad maestra debe conocer la identidad del resto de unidades que están en modo standby en su radio de cobertura.

El maestro o aquella unidad que inicia la piconet transmite el código de acceso continuamente en periodos de 10 ms, que son recibidas por el resto de unidades que se encuentran en standby.

El tren de 10 ms. de códigos de acceso de diferentes saltos de portadora, se transmite repetidamente hasta que el receptor responde o bien se excede el tiempo de respuesta.

Cuando una unidad emisora y una receptora seleccionan la misma portadora de salto, la receptora recibe el código de acceso y devuelve una confirmación de recibo de la señal, es entonces cuando la unidad emisora envía un paquete de datos que contiene su identidad y frecuencia de reloj actual. Después de que el receptor acepta éste paquete, ajustará su reloj para seleccionar el canal de salto correcto determinado por emisor. De éste modo se establece una piconet en la que la unidad emisora actúa como maestra y la receptora como esclava. Después de haber recibido los paquetes de datos con los códigos de acceso, la unidad maestra debe esperar un procedimiento de requerimiento por parte de las esclavas, diferente al proceso de activación, para poder seleccionar una unidad específica con la que comunicarse.

El número máximo de unidades que pueden participar activamente en una simple piconet es de 8, un maestro y siete esclavos, por lo que la dirección MAC (Medio del control de acceso) del paquete de cabecera que se utiliza para distinguir a cada unidad dentro de la piconet, se limita a tres bits. [2]

CAPÍTULO 4:

PROTOCOLOS EN LA ARQUITECTURA BLUETOOH.

4.1 PROTOCOLO STACK.

El último objetivo de la especificación Bluetooth es permitir las aplicaciones escritas de una manera que sea compatible la especificación de Bluetooth con los dispositivos de diferentes fabricantes. Para alcanzar esta interoperatibilidad, se manejan aplicaciones (Ej. cliente-servidor) en dispositivos alejados que deben funcionar sobre protocolos idénticos. La siguiente lista de protocolos es un ejemplo del protocolo stack (de arriba hacia abajo) que apoya una aplicación de intercambio de la tarjeta comercial: vCard >>> OBEX >>> RFCOMM >>> L2CAP >>> Baseband. Dicho protocolo stack contiene una convención interna de la representación del objeto, vCard y “over-the air” de los protocolos de transporte del resto del apilado.

Diversas aplicaciones pueden funcionar sobre diferentes apilados excesivos del protocolo. Sin embargo, cada de estos diversos apilados del protocolo utiliza una transmisión de datos común de Bluetooth y la capa física. El diagrama 4.1 muestra el protocolo stack completo de Bluetooth según lo identificado en la especificación sobre la cual las aplicaciones de interoperatibilidad entre los modelos construidos para usar Bluetooth. No todas las aplicaciones hacen uso de todos los protocolos demostrados en el diagrama 4.1. Sin embargo las aplicaciones funcionan sobre una o más rebanadas verticales de este protocolo stack. Típicamente, las rebanadas verticales adicionales están para los servicios de apoyo de la aplicación principal, como el TCS binario (especificación de control de la telefonía), o SDP (protocolo del descubrimiento del servicio). Vale la pena mencionar que el diagrama 4.1 muestra las relaciones de cómo los protocolos están utilizando los servicios de otros protocolos cuando los datos de la carga útil necesitan ser transferidos sobre el aire.

Sin embargo, los protocolos pueden también tener algunas otras relaciones entre los otros protocolos, como por ejemplo algunos protocolos como L2CAP (Protocolo lógico de adaptación y acoplamiento), TCS binario pueden utilizar LMP (protocolo del encargado del acoplamiento) cuando hay necesidad de controlar al encargado del acoplamiento.

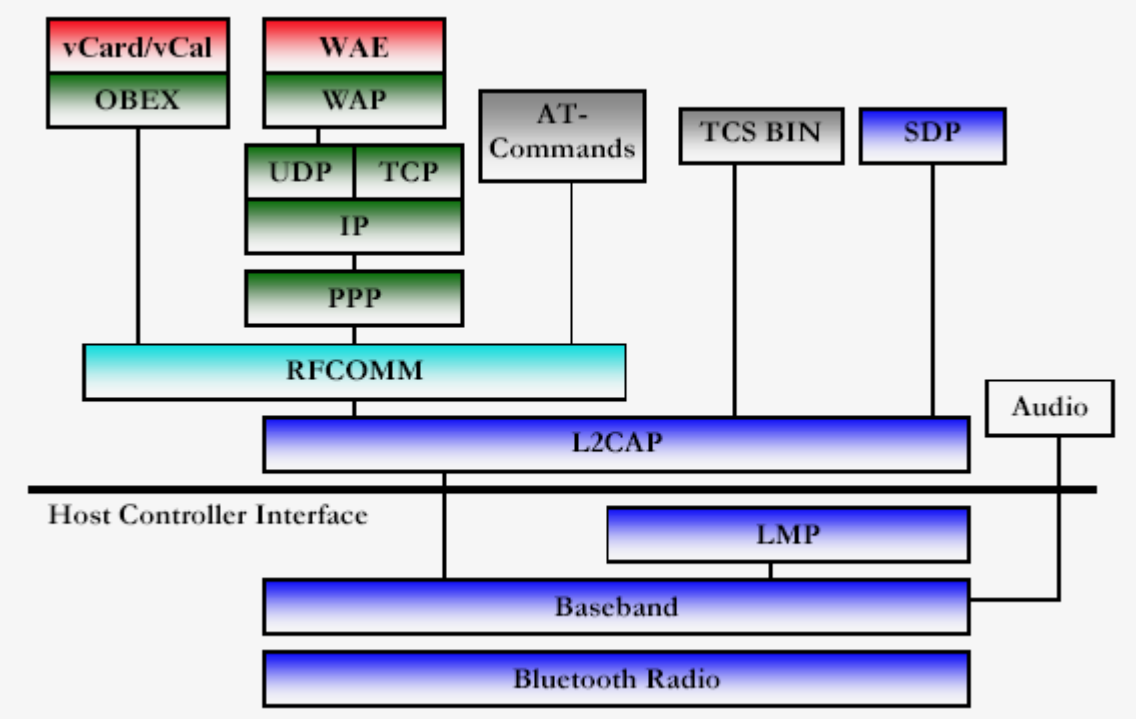

Diagrama 4.1: Representación del protocolo stack.

Como se puede ver en el diagrama 4.1, el protocolo stack completo abarca desde los protocolos de la especificación Bluetooth como LMP y L2CAP, y los protocolos que no corresponden a la especificación Bluetooth, pero que sin embargo son protocolos que complementan a la especificación Bluetooth como OBEX (protocolo del intercambio del objeto) y UDP (User Datagram Protocol). En diseñar los protocolos y el protocolo stack entero, el principio fundamental ha sido

maximizar la reutilización de los protocolos existentes para diversos propósitos en capas más altas, en vez de reinventar una nueva forma del protocolo stack.

La reutilización del protocolo también ayuda a adaptar usos existentes (la herencia) al trabajo con la tecnología de Bluetooth y a asegurar la operación y la interoperatibilidad de estas aplicaciones. Así, muchas aplicaciones desarrolladas ya por los vendedores pueden tomar la ventaja inmediata de los sistemas del hardware y de software, que son compatibles a la especificación. La especificación está también abierta lo que permite que los vendedores pongan libremente sus propios protocolos comúnmente usados en la tapa de los protocolos de la especificación Bluetooth. Así, la especificación abierta permite el desarrollo de una gran cantidad de nuevas aplicaciones que tomen la ventaja completa de las capacidades de la tecnología de Bluetooth. [6]

4.2 PROTOCOLOS BLUETOOTH.

El protocolo stack de Bluetooth se puede dividir en cuatro capas según su propósito incluyendo el aspecto si Bluetooth SIG ha estado implicado en especificar estos protocolos. Los protocolos pertenecen a las capas como se muestra en la tabla 4.1:

Protocol layer	Protocols in the stack
Bluetooth Core Protocols	Baseband [1], LMP [2], L2CAP [3], SDP [4]
Cable Replacement Protocol	RFCOMM [5]
Telephony Control Protocols	TCS Binary [6], AT-commands [7],[8],[9]
Adopted Protocols	PPP [10], UDP/TCP/IP [10], OBEX [11], WAP [12], vCard [13] , vCal [14], IrMC[1] [15], WAE [16]

Tabla 4.1: Protocolos y capas del protocolo stack Bluetooth.

Además de las capas de protocolos anteriores, la especificación también define un interfaz del regulador del anfitrión (HCI) que proporciona un interfaz del comando al regulador de la banda base al encargado del acoplamiento, y al acceso al estado de hardware y a los registros de control. En el diagrama 4.1, HCI se coloca debajo de L2CAP pero esta colocación no es obligatoria pero HCI puede existir sobre L2CAP.

Los protocolos de la base de Bluetooth abarcan exclusivamente los protocolos de la especificación Bluetooth desarrollados por los SIG de Bluetooth. RFCOMM (Protocolo de emulación de cable serial) y el protocolo binario del TCS tienden a ser desarrollados por los SIG de Bluetooth pero se basan en los TS 07.10 de ETSI y la recomendación Q.931 de ITU-T (International Telecommunication Union.) respectivamente. Los protocolos de la base de Bluetooth (más la radio de Bluetooth) son requeridos por la mayoría de los dispositivos de Bluetooth, mientras que el resto de los protocolos se utiliza solamente según lo necesitado.

Junto a la capa del reemplazo del cable, la capa del control de la telefonía y los protocolos adoptados de la forma application-oriented (se debe de interpretar como cualquier capa de protocolos la cual corra sobre la especificación Bluetooth de transporte) de la capa del protocolo permitiendo a las aplicaciones funcionar sobre los protocolos de la base de Bluetooth. Según lo mencionado anteriormente, la especificación Bluetooth son los protocolos abiertos y adicionales como por ejemplo puede ser acomodados de una manera ínter operable sobre los protocolos de la especificación Bluetooth del transporte o sobre de los protocolos application-oriented mostrados anteriormente en el diagrama 4.1.

4.3 PROTOCOLOS ESENCIALES DE BLUETOOTH.

4.3.1 Banda Base.

La banda base y la capa del control del acoplamiento permite el acoplamiento físico del RF entre las unidades de Bluetooth que forman una piconet. Pues el sistema de Bluetooth RF es un sistema de Salto de Frecuencia de Espectro disperso en el cual los paquetes se transmiten en ranuras de tiempo definidas en frecuencias definidas, esta investigación de las aplicaciones de la capa y procedimientos de la paginación para sincronizar la frecuencia de la transmisión y el reloj de diversos dispositivos de Bluetooth.

Proporciona dos clases de acoplamientos físicos con sus paquetes correspondientes de la banda base, sincronos (SCO) y asincrónico (ACL) que se puedan transmitir de una manera de la multiplexación en el mismo acoplamiento del RF. Los paquetes ACL se utilizan para los datos solamente, mientras que el paquete SCO puede contener audio solamente o una combinación del audio y de los datos. Todos los paquetes de audio y de datos pueden proporcionar diversos niveles de corrección de error como FEC (corrección de error delantero) o el CRC (chequeo de redundancia cíclico) y pueden ser cifrados.

Además, los diversos tipos de datos incluyendo mensajes de la gerencia del acoplamiento y del control son cada uno asignado a un canal especial.

4.3.2 Audio.

Los datos de audio se pueden transferir entre unos o más dispositivos de Bluetooth, haciendo varios modelos de diferentes compañías uso de datos y audio en paquetes de SCO se encaminan directamente a y desde banda base y no pasan con L2CAP. El modelo de audio es relativamente simple dentro de Bluetooth; cualquier modelo entonces no importando el fabricante puede enviar y recibir datos y audio entre uno y otro. [6]

4.3.3 Link Manager Protocol (LMP).

El protocolo encargado del acoplamiento es responsable del acoplamiento de la estructuración entre los dispositivos de Bluetooth. Esto incluye aspectos de la seguridad como la autentificación y cifrado generado; intercambiando y comprobando las llaves del acoplamiento, el cifrado, el control y la negociación de los tamaños de los paquetes de la banda base.

Además controla los modos de la energía y los ciclos de los dispositivos de radio Bluetooth y los estados de la conexión de una unidad de Bluetooth en una piconet. [7]

4.3.4 Protocolo Lógico de Adaptación y Acoplamiento (L2CAP).

El acoplamiento lógico de Bluetooth controla y el protocolo de la adaptación (L2CAP) adapta protocolos de capas superiores sobre la banda base. Puede ser pensado para trabajar en paralelo a LMP en diferencia que L2CAP proporciona servicios a la capa superior cuando los datos de la carga útil nunca se envían en los mensajes de LMP.

L2CAP proporciona servicios de conexión orientada y sin conexión orientada de los datos a los protocolos de capa superiores de capacidad de la multiplexación del protocolo, segmentación del nuevo ensamble y las abstracciones del grupo. L2CAP permite el nivel más alto a los protocolos y aplicaciones para transmitir y recibir los paquetes de los datos de L2CAP hasta 64 kilobytes en longitud.

Aunque el protocolo de la banda base proporciona los tipos del acoplamiento de SCO y ACL, L2CAP se define solamente para los acoplamientos del ACL y no se especifica ninguna ayuda para los acoplamientos de SCO en la especificación Bluetooth. [8]

4.3.5 Protocolo de Descubrimiento del Servicio (SDP).

El protocolo de descubrimiento del servicio (SDP) es parte crucial del marco de Bluetooth. Estos servicios proporcionan la base para todos los modelos usados por los diferentes fabricantes.

Usando el SDP la información del dispositivo y las características de los servicios pueden ser preguntadas y después de eso realizarse una conexión entre dos o más dispositivos de Bluetooth. El SDP se define en la especificación del protocolo del descubrimiento del servicio. [9]

4.4 PROTOCOLO DE REEMPLAZO DE CABLE.

4.4.1 Protocolo de Emulación de Cable Serial (RFCOMM).

RFCOMM es un protocolo de emulación de línea en serie y se basa en la especificación ETSI 07.10. Este protocolo de reemplazo del cable emula el control RS-232 y la banda base excesiva de Bluetooth de las señales de los datos, proporcionando a ambos capacidades de transporte para servicios superiores que usan línea de serie como mecanismo del transporte como por ejemplo al protocolo OBEX. [10]

4.5 PROTOCOLO DE CONTROL DE TELEFONÍA.

4.5.1 Protocolo de Control de Telefonía-Binario (TCS).

Protocolo del control de la telefonía - binario (TCS binario), un bit del protocolo define el control de la llamada para el establecimiento del discurso entre los dispositivos Bluetooth. Además define procedimientos de dirección de movilidad para manejar grupos de dispositivos del TCS de Bluetooth.

El TCS binario se especifica en el protocolo de control de telefonía Bluetooth. Especificación binaria que se basa en la recomendación Q.931 del ITU-T (Unión de Telefonía Internacional), aplicando las provisiones simétricas según lo indicado en el anexo D del control de la telefonía Q.931. [11]

4.5.2 Control de Telefonía-AT Commands.

Bluetooth SIG ha definido el sistema AT-COMMANDS por lo cual un teléfono móvil y un módem se pueden controlar en múltiples modelos usados por diferentes fabricantes. En Bluetooth los AT-COMMANDS que se utilizan se basan en la recomendación V.250 de la ITU y ETS 300 916 (GSM 07.07). [12]

4.6 PROTOCOLOS ADOPTADOS.

4.6.1 Protocolo Punto a Punto (PPP).

En la tecnología de Bluetooth, PPP esta designado para correr sobre RFCOMM para lograr conexiones punto a punto. El PPP esta en el protocolo IETF (Internet Engineering Task Force). El PPP establece una red de los medios que toma de la IP y la capa del PPP y los coloca sobre la LAN (Red de Área Local). [13]

4.6.2 TCP/UDP/IP (Transport Control Protocol/User Datagram Protocol/Internet Protocol)

Estos estándares de estos protocolos son definidos por el Internet Engineering Task Force (IETF) y utilizados para la comunicación a través del Internet. Actualmente es considerada como la familia de protocolos mas usada en el mundo, los stacks de TCP/IP han aparecido en numerosos dispositivos incluyendo impresoras, computadoras, teléfonos celulares, etc. El acceso a estos protocolos es independiente del sistema operativo, aunque tradicionalmente se usa un enlace que programa un modelo de la interfase. La implementación de estos estándares en los dispositivos de Bluetooth permite la comunicación con cualquier otro dispositivo conectado con el Internet. El dispositivo de Bluetooth debe ser un microteléfono celular o un punto de acceso de datos y puede ser utilizado como un puente para el Internet. TCP/IP/PPP se utiliza para todos los panoramas del uso del puente de Internet en Bluetooth y para OBEX (Protocolo de Intercambio de Objeto) en las versiones futuras. UDP/IP/PPP está también disponible como transporte para WAP (Protocolo de Conexión Inalámbrica). [14]

4.6.3 OBEX (Protocolo de Intercambio de Objeto).

El protocolo IrOBEX (shortly OBEX) es un protocolo de sesión desarrollado por la asociación infrarroja de datos (IrDA) para intercambiar objetos de una manera simple y espontánea. OBEX, que proporciona la misma funcionalidad básica que el HTTP (Protocolo de transferencia de texto) pero en una manera mucho más ligera, utiliza un modelo cliente-servidor y es independiente del mecanismo y del transporte API (Aplicación de programación de interfase), con tal que realice una base confiable del transporte.

OBEX también proporciona un modelo para representar objetos y operaciones. Además, el protocolo de OBEX define un objeto de carpeta-listado, que se utiliza para hojear el contenido de carpetas en el dispositivo alejado.

En la primera fase, RFCOMM se utiliza como capa de transporte única para OBEX. Las puestas en práctica futuras son probables apoyar también TCP/IP como capa de transporte. [15]

4.6.3.1 vCard y vCalendar.

El vCard y vCalendar son especificaciones abiertas desarrolladas por el consorcio versit y ahora controladas por el Consorcio de correo del Internet. Estas especificaciones definen el formato de una tarjeta comercial electrónica y las entradas del calendario personal respectivamente. vCard y vCALENDAR no definen ningún mecanismo del transporte sino solamente el formato bajo el cual se transportan los datos. Adoptando el vCard y vCalendar, la SIG ayudará más a promover el intercambio de la información personal debajo de éstas definiciones y apoyar formatos. El vCard y las especificaciones vCalendar están disponibles en consorcio del correo del Internet y están siendo desarrolladas más a fondo por el Internet Engineering Task Force (IETF).

Otros formatos que son transferidos por OBEX en Bluetooth, son el vMessage y el vNote. Estos formatos son también estándares abiertos y se utilizan para intercambiar mensajes y notas. Se definen en la especificación de IrMC (Comunicación móvil infrarroja), que también define un formato para los archivos troncales que son necesarios al sincronizar datos entre los dispositivos. [16]

4.7 WAP (PROTOCOLO DE APLICACIÓN INALÁMBRICA)

El protocolo de aplicación inalámbrica (WAP) esta trabajando para construir una red inalámbrica para que puedan trabajar en ella diferentes tecnologías. La meta es darle más volumen al ancho de banda de la Internet y la telefonía para teléfonos portátiles digitales y a otras terminales inalámbricas. En el diagrama 4.2 se muestra como funciona el protocolo de aplicación inalámbrica.

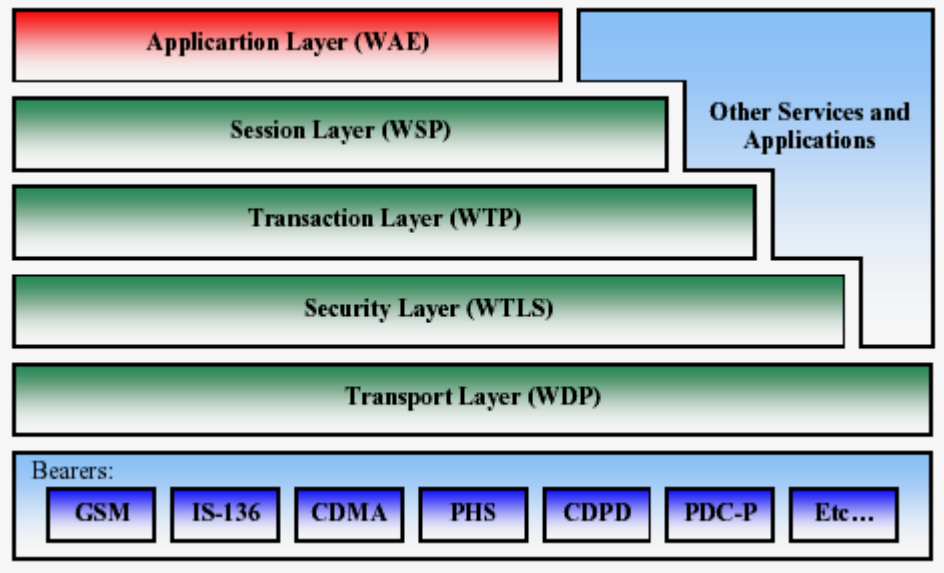

Diagrama 4.2: WAP.

La idea detrás de la opción de WAP es reutilizar los usos superiores del software desarrollados para WAE (Ambiente de Aplicación inalámbrica). Éstos incluyen los browsers de WML (Idioma inalámbrico) y de WTA que pueden actuar recíprocamente con aplicaciones en la PC. Construyendo aplicaciones de entrada entre servidores WAP y alguna otra aplicación en la PC es posible la implementación de funciones en la informática oculta como seria el control remoto

y el intercambio de datos de una computadora a un teléfono celular. El marco de WAP también abre la posibilidad de aplicaciones para teléfonos móviles que utilizan WML, tomando a WML como una escritura universal. [17]

CAPÍTULO 5:

PERFILES Y ESTÁNDARES BLUETOOTH.

5.1 PERFILES EN BLUETOOTH.

Los perfiles son una parte muy importante en la tecnología Bluetooth. Los perfiles le proveen a Bluetooth una significante ventaja sobre las otras tecnologías. Los perfiles, definidos por Bluetooth SIG, tienen la intención de asegurar la interoperatibilidad entre las aplicaciones de Bluetooth y los dispositivos de diferentes fabricantes. Estos perfiles definen los roles y capacidades para aplicaciones especificas. Diferentes perfiles pueden abarcar diferentes capas y protocolos y para diferentes grados de seguridad. Además de los requerimientos de interoperatibilidad, los protocolos pueden definir servicios requeridos para otras aplicaciones o para usuarios finales.

Todos los dispositivos Bluetooth deberán soportar el GAP (Perfil de acceso genérico) como mínimo. Este perfil en particular define el descubrimiento o hallazgo de dispositivos, procedimientos de conexión y procedimientos para varios niveles de seguridad. También se describen algunos requerimientos de interfase al usuario. Otro perfil universal, aunque no es requerido, es el SDAP (Perfil de acceso a descubrimiento de servicios) el cual define los protocolos y parámetros asociados requeridos para accesar a los perfiles.

Un número de perfiles han sido definidos incluyendo SPP (Perfil de puerto serial) y el GOEP (Perfil de intercambio de objeto genérico), TCS, RFCOMM y OBEX. Algunos de estos requieren la implementación de otros, y todos ellos requieren la implementación de perfiles genéricos. [18]

5.1.1 Perfil de Acceso Genérico (GAP).

El GAP mantiene la base de todos los perfiles que maneje Bluetooth y define los medios para establecer un eslabón entre la banda base y dispositivos Bluetooth. Además de esto, el GAP define lo siguiente:

*Las características que deben tener todos los dispositivos Bluetooth.

* Los procedimientos genéricos por descubrir y enlazarse a los dispositivos Bluetooth.

* La terminología básica para el uso de la interfase.

El GAP asegura un grado alto de interoperatibilidad entre las aplicaciones y dispositivos. También hace más fácil el diseño para definir nuevos perfiles que puedan trabajar con definiciones ya existentes.

El perfil (GAP) define funcionamientos que son genéricos y pueden ser usados por perfiles y dispositivos que llevan a cabo funciones relacionadas con el perfil GAP y con perfiles de múltiples funciones. El GAP asegura que cualquier dispositivo Bluetooth, sin tener en cuenta el fabricante y la aplicación, puedan intercambiar información. Bluetooth habilita la posibilidad para que todos los dispositivos cuenten con el perfil GAP para que puedan asegurar interoperatibilidad y co-existencia entre ellos, no importando la aplicación del dispositivo o marca del fabricante. [18]

5.1.2 Perfil de Intercambio Genérico (GOEP).

El perfil GOEP es usado para transferir un objeto de un dispositivo a otro. El objeto puede ser cualquier objeto como una fotografía, un documento, una tarjeta comercial, etc. El perfil define dos papeles, un servidor que proporciona la forma de la situación cuando un objeto es enviado o mandado, así como un cliente que comienza la acción. Las aplicaciones que usa GOEP asumen los vínculos y los canales que son establecidos y definidos por el perfil GAP. El GOEP es dependiente del SPP (Perfil del puerto serial).

El perfil GOEP mantiene un estándar genérico para otros perfiles que usan el protocolo OBEX y define el cliente y los papeles del servidor para los dispositivos. Como con todas las transacciones de OBEX; el perfil GOEP estipula al cliente para que comience a realizar todas las transacciones.

El perfil no lo hacen en esencia, sin embargo, describe cómo las aplicaciones deben definir los objetos para su intercambio y también define cómo las aplicaciones deben llevar a cabo ese intercambio exactamente, estas aplicaciones son realizadas por los perfiles que dependen de GOEP, como por ejemplo el perfil OPP (Perfil de envío de objeto), FTP (Perfil de transferencia de archivos) y SYNC (Perfil de sincronización). Bluetooth usa el perfil GOEP en dispositivos como PC's, PDA´s, teléfonos celulares entre otros. [18]

5.1.3 Perfil de Transferencia de Archivos (FTP).

El perfil de transferencia de archivo (FTP) ofrece la capacidad de transferir datos a partir de un dispositivo como puede ser desde un teléfono celular, PDA`s, computadoras, etc., a otro. Los tipos de datos incluyen, pero no se limitan a los archivos con extensión .xls, ppt, wav, jpg y .doc. También, este modelo ofrece una posibilidad para observar el contenido de las carpetas en un dispositivo alejado.

En el diagrama 5.1 se muestra, el protocolo stack requerido para la aplicación de transferencia de archivos. La figura no muestra el LMP, la banda base, y las capas de radio aunque estas se utilizan debajo.

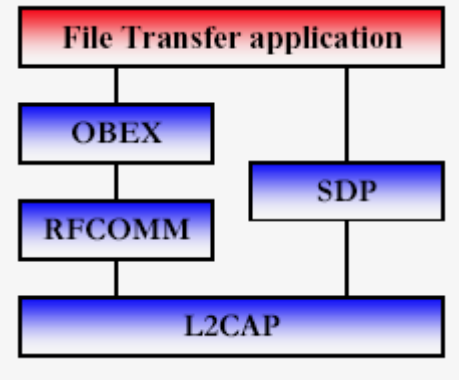

Diagrama 5.1: Protocolo Stack para la Aplicación de Transferencia de Archivos

5.1.4 Perfil del Puerto Serie (SPP).

El perfil SPP define la estructuración de los puertos seriales virtuales y conecta dos dispositivos Bluetooth. El SPP es basado en la especificación ETSI TS07.10 y usa el protocolo de RFCOMM para proporcionar emulación al puerto serie.

También el perfil SPP mantiene un reemplazo inalámbrico para la existencia del puerto serie RS-232 basado en la aplicación de comunicación serial y en el control de las señales. SPP proporciona la base para el DUN (Perfil de gestión de redes por vía telefónica), FAX, HSP (Perfil auricular). El perfil SPP soporta una velocidad de transmisión de datos de 128 Kbit/seg. Y es dependiente del perfil genérico GAP.

5.1.5 Perfil de Acceso al Descubrimiento del Servicio (SDAP).

El perfil SDAP describe cómo una aplicación debe usar el protocolo SDP (Protocolo del descubrimiento del servicio) para descubrir servicios en un dispositivo remoto, como el requerido por el GAP, cualquier dispositivo Bluetooth debe poder conectarse a cualquier otro dispositivo Bluetooth. Basado en esto, el SDAP requiere que cualquier aplicación pueda averiguar qué servicios están disponibles en cualquier dispositivo Bluetooth al que se desea conectar. [18]

El perfil maneja la búsqueda para conocer y especificar los servicios así como la búsqueda de servicios generales. SDAP involucra una aplicación, el servicio descubre al usuario de la aplicación que es requerida en un dispositivo de Bluetooth para localizar servicios. Esta interfase de aplicación con el SDP envía y recibe preguntas de uno y otro dispositivo Blutooth. SDAP depende del GAP.

5.1.6 Perfil de Gestión de Redes por Vía Telefónica (DUN).

El perfil DUN proporciona una norma para acceder al Internet y otros servicios que utilizan la vía telefónica para acceder a ellos sobre la tecnología de Bluetooth. El escenario más común es el acceso a Internet desde una laptop por modem inalámbrico. Es basado en SPP y mantiene conversión relativamente fácil de productos existentes, a través de los muchos rasgos que tienen en común con los protocolos alambricos que realizan la misma tarea. Éstos incluyen el comando AT especificado en ETSI 07.07 y PPP.

Como otros perfiles construidos sobre el perfil SPP, el eslabón de serie virtual creado por las capas más bajas del Bluetooth la pila protocolar es transparente para las aplicaciones que usan el perfil DUN. Así, el driver del módem en la terminal del modem está comunicando sobre la tecnología de Bluetooth. La aplicación en el modem es comúnmente sorprendida y no se puede conectar con el gateway. [18]

El perfil DUN describe dos papeles, el gateway y los dispositivos terminales. El gateway mantiene acceso a la red al dispositivo terminal. Una configuración típica consiste en una acción telefónica móvil como el gateway para una computadora personal que actúa como el papel terminal.

5.1.7 Perfil de Envío de Objeto (OPP).

El perfil OPP define los papeles del envío del servidor y del envío del cliente. Estos papeles son análogos y deben ser ínter operables con el servidor y el cliente. Se llama envío porque los traslados siempre son promovidos por el remitente (cliente) y no por el receptor (servidor). El OPP enfoca en un rango estrecho de formatos del objeto para aumentar al máximo la interoperatibilidad. El formato aceptado comúnmente es el vCard. OPP también puede usarse para enviar objetos como imágenes o texto. [18]

5.1.8 Perfil de Sincronización (SYNC).

El perfil de la sincronización se usa junto con GOEP para habilitar sincronización de calendario e información de dirección (gerente de información personal (PIM) entre los dispositivos Bluetooth. El perfil también describe cómo una aplicación puede apoyar a una sincronización automatizada. Una aplicación común de este perfil es el intercambio de datos entre un PDA y computadora. La SYNC define el cliente y los roles del servidor. [19]

5.2 ESTÁNDAR IEEE.

Durante la ultima semana del mes de marzo del 2002 la IEEE aprobó finalmente el estándar IEEE 802.15.1 compatible totalmente con la tecnología Bluetooth v1.1. En este estándar se definen las especificaciones de la capa física y MAC (control de acceso al medio) para las redes WPANs. El nuevo estándar permitirá una mayor validez y soporte en el mercado de las especificaciones de Bluetooth, además es un recurso adicional para aquellos que implementen dispositivos basados en esta tecnología.

Anteriormente a la estandarización, dispositivos Bluetooth no podían coexistir con los dispositivos basados en IEEE 802.11b debido a que ambos se interferían entre sí. Otro esfuerzo importante para buscar la interoperatibilidad entre dos sistemas lo están haciendo la compañía Intersil Corp., fabricante de chips para el protocolo IEEE 802.11b (Wi-Fi) y la compañía Silicon Wave Inc. fabricante de sistemas de radio de Bluetooth. Este esfuerzo entre Wi-Fi y Bluetooth es conocido como Blue802 y permitirá la operación simultánea de estos dos protocolos inalámbricos. La tecnología Blue802 fue demostrada con éxito en el pasado evento Networld+Interop 2002 en las Vegas. [20]

CAPÍTULO 6:

SEGURIDAD Y APLICACIONES BLUETOOTH.

6.1 SEGURIDAD.

En el mundo sin hilos de hoy, la seguridad significa que los datos que se están enviando entre nosotros invisiblemente ya sea de dispositivo a dispositivo, de país a país o de persona a persona sean seguros y confiables. Estos datos en forma de e-mail, fotos, contactos y direcciones son precisas y privadas para cada uno de nosotros. Esta información privada necesita ser enviada con seguridad a su recipiente previsto sin la interceptación. Estándares inalámbricos que todo el mundo está desarrollando y que tiene varios formatos para ocuparse de las aplicaciones de seguridad de sus usuarios. La tecnología Bluetooth no es ninguna excepción ya que ha puesto gran énfasis en seguridad inalámbrica de modo que los usuarios de este estándar global puedan sentirse seguros mientras que hagan sus conexiones.

El grupo de interés especial Bluetooth (SIG), compuesto por 4000 fabricantes tiene un grupo de expertos en la seguridad de Bluetooth, compuesto de ingenieros que proporcionan información y diseñan nuevas formas de seguridad para que la tecnología de Bluetooth sea confiable y segura de intercepciones. Los fabricantes de dispositivos con tecnología Bluetooth ofrecen varias opciones de seguridad. [21]

6.1.1 Modos de Seguridad.

Hay tres modos de seguridad para el acceso de Bluetooth entre dos dispositivos:

Modo 1: modo no seguro.

Modo 2: modo hecho cumplir.

Modo 3: seguridad hecha cumplir.

El fabricante de cada producto determina estos modos de la seguridad. Los dispositivos y los servicios también tienen diversos niveles de seguridad. Para los dispositivos, hay dos niveles: dispositivo confiable y dispositivo no confiable. Un dispositivo confiable, siendo apareado con otro dispositivo tiene acceso sin restricción a tiene acceso a todos los servicios.

Con respecto a los servicios hay tres niveles de seguridad: servicios que requieren la autorización y la autentificación, servicios que requieren la autentificación solamente y servicios que están abiertos a todos los dispositivos.

Últimamente la información falsa acerca de la seguridad de la tecnología Bluetooth ha aumentado. [21]

Los modos de seguridad actuales implican típicamente a los teléfonos móviles. Estos modos de seguridad también se aplican a otras clases de dispositivos. El algoritmo del cifrado en las especificaciones de Bluetooth es seguro. Esto permite que dispositivos tales como ratones y los teclados se conecten con una PC, un teléfono móvil se sincronice con una PC y un PDA pueda usar un teléfono móvil como un módem, por nombrar apenas algunos de muchos casos.

The Bluetooth SIG trabaja en conjunto con sus miembros para investigar cualquier problema de seguridad que se divulgue para entender su causa desde la raíz. Si es un problema de la especificación Bluetooth, los miembros de la SIG trabajan para corregir el problema y así asegurar a los dispositivos futuros para que no sufran de la misma vulnerabilidad; esto es un proceso continuo. Los problemas recientemente descubiertos son provocados por jackers avanzados que acceden a la información almacenada en los teléfonos móviles usando ilegalmente la aplicación de Bluetooth. Los nombres bluesnarfing y bluebugging se han dado a estos métodos de acceso ilegal e incorrecto a la información. [21]

6.2 VIOLACIONES A LA SEGURIDAD.

6.2.1 Bluejacking.

Bluejacking permite que los usuarios telefónonicos envíen las tarjetas comerciales anónimamente usando la tecnología inalámbrica Bluetooth. Bluejacking no implica el retiro o la alteración de ningún de los datos del dispositivo.

Estas tarjetas comerciales tienen a menudo un mensaje inteligente o coqueto en lugar del nombre típico y número de teléfono. Bluejackers buscan a menudo el teléfono receptor de un usuario vulnerable. Los Bluejackers envían un mensaje a ese dispositivo invitándolo a conectarse para intercambiar información, los usuarios telefónicos que reciben un mensaje del bluejacker deben negarse a agregar el mensaje a sus contactos o a su libro de dirección para no ser victimas de un robo de datos. Para llevar a cabo un bluejacking los dispositivos deben estar dentro de una distancia de 10 metros. Los dispositivos que se fijan en modo anónimo no son susceptibles al bluejacking. [21]

6.2.2 Bluebugging.

Bluebugging permite que los individuos expertos tengan acceso a los comandos del teléfono móvil usando la tecnología inalámbrica de Bluetooth sin la notificación o alertar al usuario del teléfono. La vulnerabilidad permite que el jacker inicie llamadas telefónicas, envíe y reciba mensajes de texto, lea y escriba contactos del directorio telefónico, escuche conversaciones telefónicas y puede también conectarse a Internet.

Como con todos los ataques a dispositivos con tecnología Bluetooth el jacker debe estar dentro de una gama de 10 metros del teléfono. Lo cual significa una vulnerabilidad separada de bluesnarfing y no afecta a todos los teléfonos como bluesnarfing. [21]

6.2.3 Bluesnarfing.

Bluesnarfing permite que los jackers accedan a los datos almacenados en un teléfono usando la tecnología inalámbrica Bluetooth sin alertar al usuario del teléfono de la conexión hecha al dispositivo. La información que se puede alcanzar de este modo incluye el directorio telefónico, las imágenes asociadas, el calendario, y el IMEI (identidad móvil internacional del equipo).

Fijando el dispositivo en no descubierto, se convierte considerablemente más difícil de encontrar y de atacar al dispositivo. Sin el equipo especializado el jacker debe estar dentro de una gama de 10 metros del dispositivo mientras que funciona un dispositivo con software especializado. [21]

6.2.4 Es Bluetooth Susceptible a los Jackers de Otras Maneras.

Actualmente los ataques antes mencionados son las únicas posibilidades conocidas por contar con una cantidad limitada de productos en el mercado, si las medidas apropiadas se toman por ejemplo usar códigos razonablemente largos del código PIN (Numero de Identificación Personal) o el apareamiento de los dispositivos en privado. El SIG de Bluetooth continúa estudiando los riesgos de la seguridad asociados a la tecnología y determinando su viabilidad mientras que la tecnología se extiende y se desarrolla. [21]

6.3 FORMAS DE SEGURIDAD CONTRA LOS JACKERS.

Los consumidores pueden hacer un número de cosas para proteger sus datos. Si los usuarios tienen un teléfono que sea vulnerable a bluesnarfing o a bluebugging, deben entrar en contacto con el fabricante del teléfono o llevar el teléfono un punto de servicio autorizado por el fabricante. Los fabricantes de los dispositivos vulnerables han desarrollado remiendos del software para fijar la vulnerabilidad. Además, si los usuarios se encuentran en modo descubierto pueden dar vuelta al dispositivo al modo no descubierto y no usar la tecnología inalámbrica Bluetooth en áreas desconocidas. Los usuarios pueden también asegurar sus datos no apareándose con los dispositivos desconocidos. Si un usuario recibe una invitación de aparearse con otro dispositivo y se le pide pedido su código PIN el usuario no debe aparearse. Es siempre recomendable aparearse con dispositivos en áreas privadas. Evitar aparear sus dispositivos en lugares públicos. [21]

6.3.1 Código PIN.

El número de identificación personal (PIN) son cuatro dígitos o más dígitos alfanuméricos para un apareamiento seguro. Se recomienda que los usuarios empleen un mínimo de ocho dígitos para el código PIN o más dígitos alfanuméricos si es posible. Los dueños del dispositivo deben solamente compartir su código PIN con individuos y dispositivos confiables. Sin el código PIN el apareamiento no puede ocurrir.

Un jacker puede supervisar y registrar actividades en el espectro de la frecuencia y después utilizar teóricamente una computadora para regenerar los dígitos del código del PIN. Esto requiere el hardware especialmente construido y el conocimiento cuidadoso de los sistemas de Bluetooth. Usando un código PIN con ocho o más dígitos alfanuméricos le tomaría al jacker algunos años para descubrir el código PIN, pero usando un código PIN de cuatro dígitos numéricos, el jacker podría descubrir el código PIN en cuestión de algunas horas, para poder lograr esto el jacker requiere de software especializado.

Los dispositivos de Bluetooth generan una conexión segura por medio del proceso de apareamiento inicial. Durante este proceso uno o ambos dispositivos necesitan un código PIN para poder iniciar una serie algoritmos internos para generar una llave segura para autentificar a los dispositivos que se conecten en el futuro. Un papel académico nuevo propone un proceso teórico que podría potencialmente revolucionar los ajustes de la seguridad en los dispositivos Bluetooth. Para hacer esto el dispositivo que ataca necesitaría interceptar el proceso de apareamiento inicial, desde este punto puede utilizar un algoritmo para descifrar la llave de seguridad.

El equipo necesitado para este proceso es muy costoso; si este proceso tiene éxito el usuario verá un mensaje en su dispositivo que pida que vuelvan a ingresar el código PIN, si el usuario hace esto mientras que el atacante esta presente y el código PIN que introducen es muy corto, entonces el ataque podría tener éxito teóricamente. Si la llave de seguridad del código PIN es solo de cuatro dígitos numéricos, una PC rápida puede calcular la llave de la seguridad en menos de una décima de un segundo.

Mientras que si la llave del código PIN consta de ocho caracteres alfanuméricos le tomaría al jacker descifrar la llave de seguridad cientos años lo que hace casi imposible que el jacker consiga descifrar la llave de seguridad. [21]

6.3.2 Puede The Bluetooth SIG Garantizar la Seguridad.

La seguridad absoluta no se puede garantizar totalmente, la seguridad es un esfuerzo en curso e importante para cualquier tecnología. The Bluetooth SIG ha hecho de la seguridad una alta prioridad y sigue estudiando y desarrollando nuevas formas de seguridad como aislar el apareamiento es decir hacerlo privado después de la conexión. [21]

6.4 APLICACIONES DE LA TECNOLOGÍA BLUETOOTH.

Bluetooth es una especificación para la industria de la computación y telecomunicaciones que describe como se pueden interconectar dispositivos como teléfonos celulares, PDA, computadoras y muchos otros dispositivos, ya sea en el hogar, en la oficina, en el auto, etc. Utilizando una conexión inalámbrica de corto alcance.

Una aplicación importante de Bluetooth es en redes caseras. El incremento de computadores personales implica un aumento en la necesidad de instalar redes que comuniquen estas maquinas de forma sencilla y económica.

La combinación de datos sincronos y asíncronos mediante el mismo dispositivo de comunicación hace a Bluetooth ideal para su uso entre equipos de manos libres en teléfonos móviles, impresoras, faxes y la comunicación de estos dispositivos con computadores personales y PDA's.

Con la tecnología Bluetooth, se puede enviar e-mails desde una laptop hacia un teléfono celular ubicado dentro de un maletín. Su celular con enlace Bluetooth o PDA's equipados similarmente, pueden sincronizarse automáticamente con su PC en su oficina mientras esta caminando dentro del rango de Bluetooth. También puede tener un sistema de manos libres inalámbrico y un celular, o puede descargar imágenes desde una cámara digital a su PC o a un celular.

6.4.1 Ejemplos de Dispositivos con Tecnología Bluetooth.

6.4.1.1 Audífono Inalámbrico NOKIA.

Este audífono compacto esta equipado con conexión inalámbrica, que da control "manos libres" al teléfono móvil, sin la necesidad de cables.

Debido a que es una conexión inalámbrica basada en el estándar Bluetooth, este audífono es compatible con un amplio rango de teléfonos equipados con Bluetooth, cualquiera que sea el fabricante.

El equipo puede ser activado para hacer llamadas por voz. Para maximizar la seguridad de las llamadas, el equipo soporta encriptamiento de la conexión inalámbrica para teléfonos compatibles. [22] Vea Fig. 6.1:

Fig.6.1: Audífono Inalámbrico Nokia.

6.4.1.2 Consola de Juegos NOKIA N-GAGE.

La consola móvil de juegos con soporte para Bluetooth y GPRS, permite entre sus funciones: reproductor de mp3 digital, radio FM, mensajes MMS, correo electrónico y explorador XHTML. Tiene la particularidad de poder jugar en modo multi jugador, sin necesidad de cables, si no por medio de la tecnología Bluetooth. [22] Vea Fig. 6.2.

Fig.6.2: Consola de juegos Nokia N-GAGE.

6.4.1.3 Tarjeta para PALM con Tecnología Bluetooth.

La tarjeta para Palm con tecnología Bluetooth sirve para conectar inalámbricamente los dispositivos móviles entre otros dispositivos con tecnología Bluetooth ubicados en un radio de 10 metros. Se pueden conectar a otras Palm, teléfonos móviles, laptops, impresoras y a un servidor de puntos de acceso a una LAN inalámbrica. Envía mensajes SMS, planifica calendarios, envía documentos a impresoras o comparte información de manera segura sin saltos, cortes o pérdidas de datos. Vea Fig.6.3:

Fig.6.3: Tarjeta para Palm con tecnología Bluetooth.

6.4.1.4 Adaptador USB Bluetooth.

Disfrute de la libertad inalámbrica. El adaptador USB Bluetooth de Belkin le permite crear conexiones libres de cables entre su ordenador dotado de puerto USB y los dispositivos que utilizan tecnología Bluetooth. Este adaptador es compatible con dispositivos certificados Bluetooth 2.0 + EDR. Esto significa un mejor rendimiento para aplicaciones de voz y multimedia. Este moderno adaptador proporciona un amplio ancho de banda para sonido estéreo, permitiendo una mayor calidad de audio y una escucha sin interrupciones.

El adaptador Bluetooth de Belkin añade la última tecnología Bluetooth a su ordenador de sobremesa o portátil y le permite conectar de forma simultánea hasta 7 dispositivos adicionales con tecnología Bluetooth incorporada como impresoras, PDAs, teléfonos móviles o auriculares estéreo. Simplemente enchufe el adaptador al puerto USB de su ordenador y conéctelo sin esfuerzo a cualquier dispositivo con tecnología Bluetooth incorporada.

Si realmente desea potenciar los equipos de audio Bluetooth de los que dispone, este adaptador es su mejor aliado para conseguir un sistema de verdadera calidad de sonido y de una eficacia de transmisión nunca vista hasta ahora. [23] Vea Fig.6.4:

Fig.6.4: Adaptador USB Bluetooth.

6.4.1.5 Teléfono SONY ERICSSON WALKMAN W800i

El teléfono Sony Ericsson Walkman W800i almacena canciones en mp3 con una excelente calidad de sonido además incluye una cámara digital de 2 mega píxeles integrada para tomar imágenes de calidad dondequiera que esté. Abra la cubierta del objetivo activo y aparecerá el visor de la cámara del W800i en la pantalla listo para su uso.

Comparte fácilmente con Bluetooth™ e infrarrojos imágenes, vídeo y música con otro teléfono o a un PC. [24] Vea Fig.6.5:

Fig.6.5: Teléfono Sony Ericsson Walkman W800i.

CONCLUSIÓN.

En conclusión Bluetooth puede considerarse como una tecnología para redes inalámbricas pequeñas y seguras que puede proveer a los usuarios de conectividad transparente con otros dispositivos también habilitados. Debido al renombre e influencia que tienen las empresas involucradas en el desarrollo y mejoramiento de este estándar, es de esperarse que pronto la mayoría de los dispositivos personales como teléfonos celulares, PDAs, Palm, Laptop, impresoras, auto esteros, PC´s, etc. sean fabricados con tecnología Bluetooth, con lo que casi sin darnos cuenta todos seremos partícipes de un gran salto en la aplicación de la tecnología inalámbrica en la vida diaria.

La tecnología de Bluetooth a diferencia del infrarrojo te permite conectar todos tus periféricos de la oficina vía inalámbrica. Conectar tu PC o notebook con las impresoras, los scanners y los faxes sin preocuparse por los cables. Puedes aumentar tu libertad conectando tu ratón o el teclado vía inalámbrica con tu computadora. Si tus cámaras fotográficas digitales poseen Bluetooth, puedes enviar imágenes de video de cualquier localización a cualquier localización sin la molestia de conectar tu cámara fotográfica con el teléfono móvil. Bluetooth permite que tengamos teléfonos de tres vías. Cuando estás en movimiento, funciona como un teléfono móvil (uso de red celular). Y cuando tu teléfono entra en el rango de otro teléfono móvil con Bluetooth funciona como una radio (hablar entre celulares sin usar la red de telefonía móvil).

Bluetooth es adecuado para conectar dispositivos a alta velocidad, un megabyte por segundo, en distancias menores a 10 mts, para el intercambio de

información; de esta forma Bluetooth a diferencia de Wi-Fi es la manera mas barata, sencilla y cómoda para conectar dispositivos personales sin la necesidad de cables, ya que Wi-Fi tiene una rapidez de conexión 10 veces mayor a la que permite Bluetooth y con un radio de cobertura mucho más extenso, de aproximadamente 100 metros, lo que permite una buena conexión a Internet. Wi-Fi es una tecnología inalámbrica pensada para conectarse a Internet sin la necesidad de cables.

Bluetooth a partir de su versión 1.2 ofrece una solución inalámbrica para coexistir con Wi-Fi en el espectro de 2.4 Ghz. sin interferirse entre ellos. Poseer estas dos tecnologías en conjunto nos ayuda a aprovechar mejor los equipos personales.

ACRÓNIMOS.

ACRÓNIMO	**SIGNIFICADO**
ACL	Asynchronous Connection (Conexión asíncrona)
API	Application Programming Interfase (Interfase de programación de aplicación)
CRC	Cíclica Redundancy Check (Control de redundancia cíclico)
DT	Data Terminal (Terminal de datos)
FEC	Forward Error Correction (Corrección de error delantero)
FTP	File Transfer Protocol (Protocolo de transferencia de archivos)
GAP	Generic Access Profile (Perfil genérico de acceso)
GOEP	Generic Object Exchange Profile (Perfil de intercambio de objeto genérico)
HCI	Host Controller Interface (Interfaz del controlador del anfitrión)
HTTP	HyperText Transfer Protocol (Protocolo de transferencia de texto)
IETF	Internet Engineering Task Force
IP	Internet Protocol (Protocolo de Internet)
IrDA	Infrared Data Association (Asociación de datos infrarrojos)
IrMC	Ir Mobile Communications (Comunicación móvil infrarroja)
LAN	Local Area Network (Red de area local)
LAP	LAN Access Point (punto de acceso de la red de área local)
LMP	Link Manager Protocol (Protocolo de acoplamiento)
L2CAP	Logical Link and Control Adaptation Protocol (Protocolo lógico de la adaptación del acoplamiento y control)
OBEX	Object Exchange Protocol (Protocolo de intercambio de objeto)
PDA	Personal Digital Assistant (Asistente digital personal)
PIM	Personal Information Management (Gerencia de información personal)

ACRONIMO	**SIGNIFICADO**
PPP	Point-to-Point Protocol (Protocolo punto a punto)
PSTN	Public Switched Telephony Network (Red de telefonía publica)
RFCOM	Serial Cable Emulation Protocol (Protocolo de emulación de cable serial)
SCO	Synchronous Connection-Oriented (Conexión sincrona)
SDAP	Service Discovery Application Profile (Perfil del descubrimiento del servicio de la aplicación)
SDP	Service Discovery Protocol (Perfil del descubrimiento del servicio)
TCP/UDP	Transport Control Protocol/User Datagram Protocol (Protocolo de control de transporte/Protocolo de datagrama)
TCS Binary	Telephony Control Specification – Binary (Especificación del control de telefonía)
WAE	Wireless Application Environment (Aplicación inalámbrica)
WAP	Wireless Application Protocol (Protocolo de aplicación inalámbrica)
WML	Wireless Markup Language (Idioma de encarecimiento inalámbrico)
SIG	Special Interest Group
ISM	Médico-científica internacional
GFSK	Gaussian Frequency Shift Keying
FHSS	Frequency Hopping Spread Spectrum
CSVD	Modulación variable de declive delta
TDM	División de tiempo múltiplexada
FH	Salto de frecuencia
MAC	Medio del control de acceso
UDP	User Datagram Protocol

REFERENCIAS ELECTRÓNICAS.

[1] IETF, Bluetooth History,
http://www.ietf.org/proceedings/00jul/SLIDES/ipobt-agenda/sld004.htm

[2] Zona Bluetooth (2001-2002)
http://www.zonabluetooth.com/general.htm

[3] Utilicom.com, Introduction to Spread Spectrum Communications,
http://www.utilicom.com/support/spread.shtml

[5] Pearsoned.com, Bluetooth 1.1: Connect Without Cables, 2nd edition,
http://vig.pearsoned.com/samplechapter/0130661066.pdf

[17] WAP Forum, WAP Forum Specifications
(http://www.wapforum.org/what/technical.htm), July 1999

[20] (http://www.ieee.org/) 2002

[21] Zona Bluetooth Security (2001-2002)
http://www.zonabluetooth.com/general.htm

[22] http://www.nokia.com/nokia/0,1522,,00.html?orig=/bluetooth/

[23] www.belkin.com/usb

[24] www.sonyericsson.com/w800i

REFERENCIAS BIBLIOGRAFICAS.

[4] Stallings, W. (2000) *Comunicaciones y redes de computadores*.

Prentice Hall, sexta edicion Madrid.

[6] Bluetooth Special Interest Group, Baseband Specification

[7] Bluetooth Special Interest Group, LMP Specification

[8] Bluetooth Special Interest Group, L2CAP Specification

[9] Bluetooth Special Interest Group, SDP Specification

[10] Bluetooth Special Interest Group, RFCOMM with TS 07.10

[11] Bluetooth Special Interest Group, Telephony Control Protocol

Specification

[12] Bluetooth Special Interest Group, Headset Profile

[13] Bluetooth Special Interest Group, LAN Access Profile using PPP

[14] Bluetooth Special Interest Group, Fax Profile

[18] *Bluetooth* Wireless Technology Profiles

[19] Bluetooth Special Interest Group, Synchronization Profile

[15] Bluetooth Special Interest Group Object Exchange Protocol (OBEX)

[16] The Internet Mail Consortium, vCard - The Electronic Business Card Exchange Format, Version 2.1, September 1996.
The Internet Mail Consortium, vCalendar - The Electronic Calendaring and Scheduling Exchange Format, Version 1.0, September 1996.