CAPÍTULO 2: ESTÁNDAR IEEE 802.15.1 "BLUETOOTH"

2.1 Tecnología Bluetooth. Antecedentes

Con el paso del tiempo los seres humanos hemos creado tecnología la cual nos ha permitido tener una mayor comodidad en nuestras actividades o vida cotidiana es por ello que en la actualidad existe Bluetooth, que es un pequeño chip implementado en varios dispositivos electrónicos, el cual permite crear pequeñas redes de forma inalámbrica, compartir fotos, música, y videos sin la necesidad de cables, lo cual, en la actualidad es muy común entre todos nosotros.

Es por ello que varias empresas están tratando de implementar esta tecnología en sus dispositivos electrónicos, por tener la gran ventaja de olvidarse por completo de los molestos cables, lo cual es muy tentador para los usuarios que utilizan la tecnología Bluetooth, ya que pueden realizar varias conexiones a la vez sin importan su ubicación actual.

El nombre fue tomado de un rey Danés del siglo 10 llamado Harald Blatand cuya traducción al inglés seria Harold Bluetooth (diente azul, aunque es su tierra danesa significa "de tez oscura"), este rey fue famoso por sus habilidades comunicativas ya que logro la unificación de las tribus noruegas, suecas y danesas.

Bluetooth se inició a principios de 1998 con un ISG (Special Interest Group) promovido por grandes empresas como lo son Ericsson, IBM, Intel, Nokia y Toshiba, dicha tecnología se hizo pública el 20 de mayo del mismo año, la primer versión de esta tecnología fue liberada dos meses después de su publicación con la colaboración de compañías como lo son 3com, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia y Toshiba. En la figura 2.1 se muestran los diferentes dispositivos que utilizan Bluetooth.

Figura 2.1 Dispositivos Bluetooth.

2.2 Principales objetivos de Bluetooth.

- Permitir la comunicación sencilla entre dispositivos fijos y móviles.
- Evitar la dependencia de cables que permitan la comunicación.
- Permitir la creación de pequeñas redes de forma inalámbrica.
- Proveer un camino fácil para el intercambio de información.

2.3 Definición y funcionamiento de Bluetooth.

Bluetooth es una tecnología que provee un camino fácil para la comunicación entre dispositivos y conectarse a Internet a altas velocidades, sin el uso de cables. Además, se busca facilitar la sincronización de datos de computadoras móviles, teléfonos celulares y otros dispositivos.

La Tecnología Bluetooth 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.

Bluetooth está integrado en un pequeño transmisor de radiofrecuencia que permite conectar entre sí todo tipo de dispositivos electrónicos (teléfonos, ordenadores, impresoras, faxes, etc.) situados dentro de un radio limitado de 10 metros (ampliable a 100, aunque con mayor distorsión).

El transmisor está integrado en un pequeño microchip de 9x9 milímetros y opera en una frecuencia de banda global (2,4 GHz, utilizada en muchos países para usos médicos y científicos) que asegura la compatibilidad universal. Los dispositivos que incorporan Bluetooth se reconocen y se hablan de la misma forma que lo hace una computadora con su impresora. El canal permanece abierto y no requiere la intervención directa y constante del usuario cada vez que se quiere enviar algo.

El transmisor permite enviar voz y datos a una velocidad máxima de 700 Kbps. y consume un 97% menos que un teléfono móvil. Además, es inteligente: cuando el tráfico de datos disminuye el transmisor adopta el modo bajo de consumo de energía

Las diferentes partes del sistema Bluetooth son:

- Una unidad de radio
- Una unidad de control del enlace
- Gestión del enlace
- Funciones software

El sistema Bluetooth permite conexiones punto a punto y punto a multipunto. La velocidad de datos en full-dúplex dentro de una estructura como la descrita a continuación, con 10 piconets con carga máxima es de 6 Mb/s.

Siendo un piconet la colección de dispositivos (de 2 a 8) conectados por medio de la tecnología Bluetooth. Todos los dispositivos tienen la misma implementación. Sin embargo, al crearse la red una unidad actuará como maestra y el resto como esclavas mientras dure la conexión.

Controlador Bluetooth

Los niveles inferiores de la pila de protocolos Bluetooth constituyen el *controlador Bluetooth*, que contiene los bloques fundamentales de la tecnología, sobre los cuales se apoyan los niveles superiores y los protocolos de aplicación. Este componente está estandarizado y puede interactuar con otros sistemas Bluetooth de más alto nivel, aunque la separación entre ambas entidades no es obligatoria.

El nivel de radiofrecuencia (RF) está formado por el transceptor físico y sus componentes asociados. Utiliza la banda de uso no regulado a 2,4 GHz, lo que facilita la consecución de calidad en la señal y la compatibilidad entre transceptores.

Por encima suyo se encuentra el nivel de banda base (base band, BB), que controla las operaciones sobre bits y paquetes, realiza detección y corrección de errores, broadcast automático y cifrado como sus labores principales. También emite confirmaciones y peticiones de repetición de las transmisiones recibidas.

El tercer y último nivel de base es el nivel de gestión de enlace (link manager, LM), responsable del establecimiento y finalización de las conexiones, así como de su autenticación en caso necesario. También realiza el control del tráfico y la planificación, junto con la gestión de consumo y supervisión del enlace.

Anfitrión Bluetooth

El resto de niveles de base y los protocolos de aplicación residen en el anfitrión Bluetooth (también denominado host), que se comunica con el controlador utilizando una interfaz estándar. Ambas entidades pueden integrarse para su uso conjunto en sistemas empotrado, o se pueden utilizar de forma intercambiable. En cualquier caso, se asume que la capacidad de los buffers del controlador es modesta comparada con la del anfitrión, lo que puede tener consecuencias en la gestión de la calidad de servicio (quality of service, QoS) y la disponibilidad de canales, entre otros aspectos.

El nivel más importante del anfitrión es el protocolo de control y adaptación de enlace lógico (logical link control & adaptation protocol, L2CAP), encargado de controlar la comunicación proveniente de niveles superiores y la asocia a los sistemas de transporte de datos multiplexando los canales L2CAP en enlaces lógicos y segmentando las tramas adecuadamente. Puede añadir opcionalmente detección de errores y retransmisión de

paquetes a BB, así como control de flujo basado en protocolos de ventana deslizante, asignación de buffers y QoS.

Si bien estos son los componentes fundamentales de un sistema Bluetooth completo, no todos requerirán todas estas funcionalidades (en concreto, sistemas empotrados sencillos); no obstante, todo ello se define como obligatorio. A partir de aquí, las aplicaciones pueden añadir niveles de protocolo para adecuarse a funcionalidades específicas, tales como transmisión de voz o TCP/IP. Estas definiciones de perfiles están fuera del ámbito de la definición principal.

Principios operativos

El nivel físico opera en la banda ISB(Independent Side band)de uso no regulado utilizando para ello un transceptor que ejecuta saltos de frecuencia (frequency hopping) en un conjunto amplio de portadoras. Es, por tanto, un sistema de espectro de dispersión basado en saltos (frequency hopping spread spectrum), diseñado para evitar interferencias y empobrecimiento (fading) de la señal. La complejidad del hardware se acota utilizando modulación en frecuencia en su forma binaria, de forma que se alcanzan cotas de transmisión de 1 Mbps (hasta un millón de símbolos, binarios por la modulación, por segundo). Utilizando técnicas de tasa de datos mejorada (enhanced data rate) puede llegarse hasta los 2 y 3 Mbps.

Un grupo de comunicación puede compartir el canal físico con muchos otros dispositivos, por lo que se sincroniza utilizando un reloj global y un patrón de saltos específico, ambos únicos. Debe haber exactamente un dispositivo maestro que ofrece la referencia de sincronización a partir de su reloj interno; el resto de dispositivos funcionan como esclavos. El reloj del maestro y su dirección de dispositivo única definen el patrón de saltos como una permutación aleatoria de 79 frecuencias en la banda ISM. Algunas de ellas pueden no utilizarse si presentan interferencias frecuentes. Esto favorece la existencia de grupos independientes entre sí o diversas piconets que comparten un mismo canal, a la vez que aumenta la tolerancia a sistemas que no cambian nunca sus frecuencias de transmisión.

El canal físico se define a través de slots de tiempo que se utilizan para enviar paquetes entre los dispositivos. Estos envíos se realizan mediante un dúplex basado en división de tiempo (time-división dúplex), equivalente a full dúplex.

Las comunicaciones existen como resultado de la interacción entre entidades de alto nivel, que se implementan según sus propias interfaces características y comportamiento definitorio.

- El gestor de recursos de banda base (base band resource manager) controla el acceso al transceptor y planifica los accesos a los canales físicos definidos, que establece entre los dispositivos que lo solicitan. Incluye también servicios de análisis de las portadoras y los requerimientos de QoS, entre otros.

- El gestor de enlace controla los canales y transportes lógicos junto con los canales físicos; se comunica con otros gestores de enlace utilizando el protocolo de gestor de enlace. También se encarga de la calidad de servicio, el cifrado y el control de la potencia de la transmisión.

- El controlador de enlace genera los paquetes a partir del contador y los parámetros de enlace y transporte, y extrae la información de los que recibe. Realiza el control de flujo, las confirmaciones y las peticiones de retransmisión.

- El controlador de canal coopera con los controladores de enlaces tanto locales como remotos para crear canales y conexiones.

- El gestor de recursos de *L2CAP* gestiona el envío de paquetes a BB y realiza algunas verificaciones sobre los límites establecidos por QoS, si bien la arquitectura supone que las aplicaciones no intentan burlar estos límites, por lo que este control es bastante limitado.

2.4 Especificaciones.

La especificación de Bluetooth define un canal de comunicación de máximo 720Kbps con rango óptimo de 10m (opcionalmente 100m).

La frecuencia de radio 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 dúplex con un máximo de 1600 saltos/seg.

Los saltos de frecuencia se dan entre un total de 79 frecuencias con 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 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 Kbps en ambas direcciones si el enlace es simétrico.

Bluetooth se denomina al protocolo de comunicaciones diseñado especialmente para dispositivos de bajo consumo, con una cobertura baja, y basados en chips de bajo costo.

Gracias a este protocolo, los dispositivos que lo implementan pueden comunicarse entre ellos cuando se encuentran dentro de su alcance. Las comunicaciones se realizan por radiofrecuencia de forma que los dispositivos no tienen por qué estar alineados, pueden incluso estar en habitaciones separadas si la potencia de transmisión lo permite.

La clasificación de los dispositivos Bluetooth como "Clase 1", "Clase 2" o "Clase 3" es únicamente una referencia de la potencia de trasmisión del dispositivo, siendo totalmente compatibles los dispositivos de una clase con los de la otra. La tabla 2.1 muestra la clasificación de los dispositivos Bluetooth.

CLASE	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	RANGO (aproximado)
Clase 1	100	20	100 m
Clase 2	2.5	4	10 m
Clase 3	1	0	1 m

Tabla 2.1 Especificaciones Bluetooth.

Cabe mencionar que en la mayoría de los casos, la cobertura efectiva de un dispositivo de clase 2 se extiende cuando se conecta a un transceptor de clase 1. Esto es así gracias a la mayor sensibilidad y potencia de transmisión del dispositivo de clase 1.

Es decir, la mayor potencia de transmisión del dispositivo de clase 1 permite que la señal llegue con energía suficiente hasta el de clase 2. Por otra parte la mayor sensibilidad del dispositivo de clase 1 permite recibir la señal del otro pese a ser más débil.

La tabla 2.2 muestra los diferentes anchos de banda de Bluetooth.

Versión	Ancho de banda
Versión 1.2	1 Mbps
Versión 2.0 + EDR	3 Mbps
UWB Bluetooth (propuesto)	53 - 480 Mbps

Tabla 2.2 Ancho de banda Bluetooth.

2.5 Arquitectura de Software y Hardware.

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).(Ver figura 2.2).

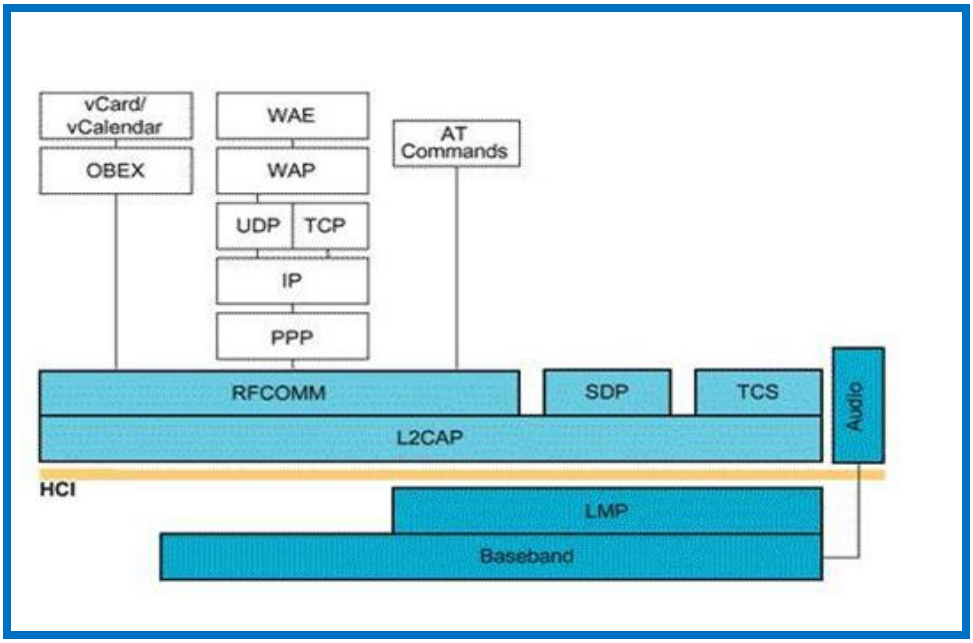

Figura 2.2 Interfaz de host del controlador.

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 re ensamblaje de los paquetes para poder enviar paquetes de mayor tamaño a través de la conexión Bluetooth.

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 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 cifrado 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. La figura 2.3 muestra la arquitectura de harware Bluetooth.

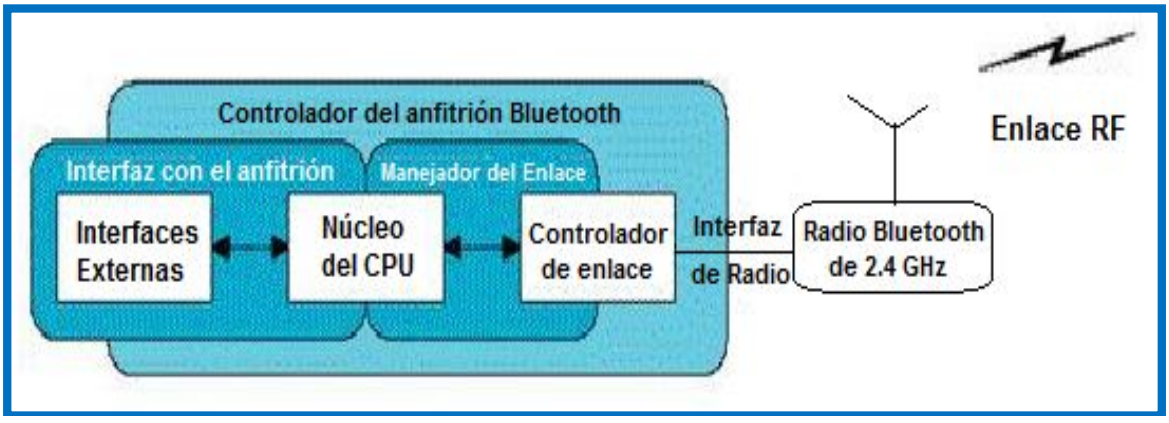

Figura 2.3 Arquitectura de Hardware Bluetooth.

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.
- Autenticación.
- Negociación y determinación de tipos de enlace, por ejemplo SCO o ACL
- Determinación del tipo de cuerpo de cada paquete.

2.6 Redes Bluetooth

Bluetooth ha sido diseñado para operar en un ambiente multi-usuario. El arreglo en una red Bluetooth puede ser punto a punto o punto-multipunto. En este tipo de conexiones, el canal se comparte con varias unidades. Dos o más unidades compartiendo el mismo canal forman una piconet. Cualquier unidad de una piconet, puede establecer una conexión a otra piconet para formar un conjunto de conexiones entre diversas piconets denominado Scatternet.

Las computadoras, teléfonos móviles, aparatos domésticos y equipos de oficina, basados en Bluetooth pueden conectarse entre sí dentro de áreas físicas reducidas, sin necesidad de utilizar cableado, de forma segura y barata y a altas velocidades de transmisión. También se pretende ofrecer acceso a Internet. La especificación de Bluetooth pretende que todas las aplicaciones sean capaces de operar entre sí. Para conseguir esta interoperabilidad, las aplicaciones en dispositivos remotos deben ejecutarse sobre una pila de protocolos idénticos.

Para comunicarse con otros dispositivos Bluetooth, se requiere un hardware específico para Bluetooth, que incluye un módulo de banda base, así como otro módulo de radio y una antena.

Además deberá haber un software encargado de controlar la conexión entre dos dispositivos Bluetooth; este software (Link Manager o Administrador de Enlace) por lo general correrá en un microprocesador dedicado. Los Link Managers de diferentes dispositivos Bluetooth se comunicarán mediante el protocolo LMP (Link Manager Protocol o Protocolo de Administrador de Enlace). Además habrá otros módulos de software, que constituirán la pila de protocolos, y garantizarán la interoperabilidad entre aplicaciones alojadas en diferentes dispositivos Bluetooth.

En la figura 2.4 se muestra la pila de los diferentes protocolos utilizados por Bluetooth.

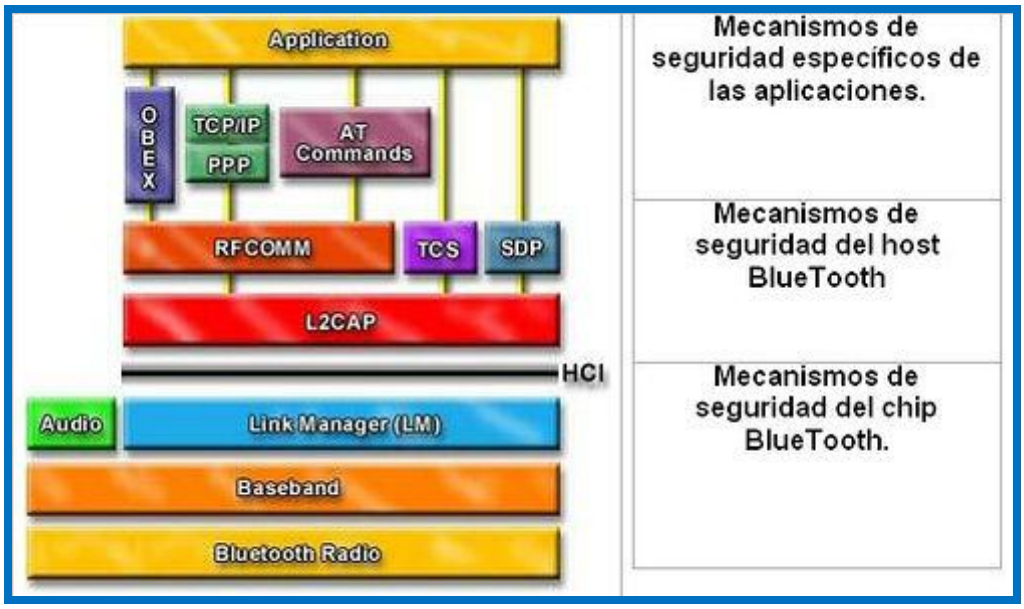

Figura 2.4 Pila de Protocolos Bluetooth

La pila completa se compone tanto de protocolos específicos de Bluetooth (LM (Link Manager) y L2CAP (Logical Link Control Adaption Protocol), por ejemplo) como de protocolos no específicos de Bluetooth como son OBEX (Objects Exchange Protocol o Protocolo de Objetos de Intercambio), UDP (User Datagram Protocol o Protocolo de Datagramas de Usuario), TCP, IP, etc. Debido a que la hora de diseñar la torre de protocolos, el objetivo principal ha sido maximizar el número de protocolos existentes que se puedan reutilizar en las capas más altas para diferentes propósitos.

A parte de todos estos protocolos, la especificación define el HCI (Host Controller Interface o Interfaz de Controlador de Host), que se encarga de proporcionar una interfaz de comandos al controlador Base Band, al gestor de enlace, y nos da acceso al estado del hardware y a los registros de control.

2.6.1 Descripción de los protocolos

- **Link Manager (LM) y Link Manager Protocol (LMP).**

Link Manager.

El Link Manager es el sistema que consigue establecer la conexión entre dispositivos. Se encarga del establecimiento, la autenticación y la configuración del enlace. El Link Manager localiza a otros gestores y se comunica con ellos gracias al protocolo de gestión del enlace LMP. Para poder realizar su función de proveedor de servicio, el LM utiliza los servicios incluidos en el controlador de enlace (LC, "Link Controller").

El Link Manager Protocol básicamente consiste en un número de PDUs (Protocol Data Units o Unidades de Datos de Protocolo) que son enviadas de un dispositivo a otro.

A continuación se enuncian los servicios soportados:

- Transmisión y recepción de datos.
- Petición de nombre: El gestor de enlace tiene un eficiente método para inquirir y reportar la ID de un dispositivo con una longitud de máximo 16 caracteres.
- Petición de las direcciones de enlace.
- Establecimiento de la conexión.
- Autenticación.
- Negociación del modo de enlace y establecimiento, por ejemplo, modo datos o modo voz/datos. Esto puede cambiarse durante la conexión.

- **Interfaz de la Controladora de la Máquina (HCI).**

La interfaz de la Controladora de la Máquina (Host Controller Interface) proporciona una interfaz de comandos para la controladora de banda base y para el gestor de enlace, y permite acceder al estado del hardware y a los registros de control.

Esta interfaz proporciona una capa de acceso homogénea para todos los dispositivos Bluetooth de banda base. La capa HCI de la máquina intercambia comandos y datos con el firmware del HCI presente en el dispositivo Bluetooth. El driver de la capa de transporte de la controladora de la máquina (es decir, el driver del bus físico) proporciona ambas capas de HCI la posibilidad de intercambiar información entre ellas.

Una de las tareas más importantes de HCI que se deben realizar es el descubrimiento automático de otros dispositivos Bluetooth que se encuentren dentro del radio de cobertura que varía de acuerdo al tipo de dispositivo Bluetooth. Esta operación se denomina en consulta. De esta manera un dispositivo remoto sólo contesta a la consulta si se encuentra configurado en modo visible (discoverable mode).

BD_ADDR (Bluetooth Device Address) o es la dirección identificadora única del dispositivo Bluetooth, similar a las direcciones MAC de las tarjetas Ethernet.

Si se realiza una consulta sobre el dispositivo Bluetooth remoto, dicho dispositivo identificará nuestra computadora con la siguiente nomenclatura: "nombre.de.su.sistema", de esta manera podemos identificar de mejor manera los dispositivos que se encuentran realizando una consulta. El nombre asignado al dispositivo local se puede modificar en cualquier momento.

El sistema Bluetooth proporciona una conexión punto a punto (con sólo dos unidades Bluetooth involucradas) o también una conexión punto multipunto. En el último caso, la conexión se comparte entre varios dispositivos Bluetooth.

- **Protocolo de Adaptación y de Control de Enlace a nivel Lógico (L2CAP).**

El protocolo L2CAP (Logical Link Control and Adaptation Protocol) proporciona servicios de datos tanto orientados a conexión como no orientados a conexión a los protocolos de las capas superiores, junto con facilidades de multiplexación y de segmentación y re ensamblaje.L2CAP permite que los protocolos de capas superiores puedan transmitir y recibir paquetes de datos L2CAP de hasta 64 kilobytes de longitud.

L2CAP se basa en el concepto de canales. Un canal es una conexión lógica que se sitúa sobre la conexión de banda base. Cada canal se asocia a un único protocolo. Cada paquete L2CAP que se recibe en un canal se redirige al protocolo superior correspondiente. Varios canales pueden operar sobre la misma conexión de banda base, pero un canal no puede tener asociados más de un protocolo de alto nivel.

- **Protocolo RFCOMM (Radio Frequency Communication Protocolo o Protocolo de Comunicación por Radio Frecuencia)**

El protocolo RFCOMM proporciona emulación de puertos serie a través del protocolo L2CAP. Este protocolo se basa en el estándar de la ETSI denominado TS 07.10. RFCOMM es un protocolo de transporte sencillo, con soporte para hasta 9 puertos serie RS-232 (EIATIA-232-E). El protocolo RFCOMM permite hasta 60 conexiones simultáneas (canales RFCOMM) entre dos dispositivos Bluetooth.

Para los propósitos de RFCOMM, un camino de comunicación involucra siempre a dos aplicaciones que se ejecutan en dos dispositivos distintos (los extremos de la comunicación). Entre ellos existe un segmento que los comunica. RFCOMM pretende cubrir aquellas aplicaciones que utilizan los puertos serie de las máquinas donde se ejecutan. El segmento de comunicación es un enlace Bluetooth desde un dispositivo al otro (conexión directa).

RFCOMM trata únicamente con la conexión de dispositivos directamente, y también con conexiones entre el dispositivo y el modem para realizar conexiones de red. RFCOMM puede soportar otras configuraciones, tales como módulos que se comunican vía Bluetooth por un lado y que proporcionan una interfaz de red cableada por el otro.

- **Protocolo de Descubrimiento de Servicios (SDP).**

El Protocolo de Descubrimiento de Servicios (Service Discovery Protocol o SDP) permite a las aplicaciones cliente descubrir la existencia de diversos servicios proporcionados por uno o varios servidores de aplicaciones, junto con los atributos y propiedades de los servicios que se ofrecen. Estos atributos de servicio incluyen el tipo o clase de servicio ofrecido y el mecanismo o la información necesaria para utilizar dichos servicios.SDP se basa en una determinada comunicación entre un servidor SDP y un cliente SDP.

El servidor mantiene una lista de registros de servicios, los cuales describen las características de los servicios ofrecidos. Cada registro contiene información sobre un

determinado servicio. Un cliente puede recuperar la información de un registro de servicio almacenado en un servidor SDP lanzando una petición SDP.

Si el cliente o la aplicación asociada con el cliente deciden utilizar un determinado servicio, debe establecer una conexión independiente con el servicio en cuestión. SDP proporciona un mecanismo para el descubrimiento de servicios y sus atributos asociados, pero no proporciona ningún mecanismo ni protocolo para utilizar dichos servicios.

Normalmente, un cliente SDP realiza una búsqueda de servicios acotada por determinadas características. No obstante hay momentos en los que resulta deseable descubrir todos los servicios ofrecidos por un servidor SDP sin que pueda existir ningún conocimiento previo sobre los registros que pueda contener. Este proceso de búsqueda de cualquier servicio ofrecido se denomina navegación o browsing.

2.6.2 Modos

Establecimiento de un dispositivo al modo "sniff" (husmear). En este modo se reduce el ciclo de trabajo de una estación esclava, ya que sólo escucha cada M slots, siendo el valor de M negociado con el gestor de enlace. La estación maestra sólo puede comenzar la transmisión en tiempos/slots específicos, separados estos por intervalos regulares.

Mantenimiento de un dispositivo de enlace en espera. En modo espera, el apagado del receptor durante períodos de tiempo más largos ahorra energía. Cualquier entidad puede volver a establecer un enlace, con una latencia media de 4 segundos. Esto es definido por el gestor de enlace y manejado por el controlador de enlace.

Establecimiento de un dispositivo en modo "aparcado": Esto es útil cuando un dispositivo no necesita participar activamente en el canal, pero sí quiere permanecer sincronizado. En este modo dicha entidad "despierta" en intervalos regulares de tiempo para escuchar al canal y así poder re-sincronizarse con el resto de entidades de la piconet.

2.6.3 Perfiles

Desde que se inició la especificación de este estándar, una de las principales preocupaciones del SIG fue garantizar la interoperabilidad total entre dispositivos de distintos fabricantes, siempre y cuando éstos compartan el mismo perfil.

Los perfiles especifican cómo utilizar la pila de protocolos de Bluetooth para implementar una solución que trabaje sin problemas con las de otras marcas. En cada uno se establecen opciones y parámetros, además de detallar cómo usar los distintos procedimientos de los diversos estándaresque se encuentren implicados.

En la figura 2.5 se muestra la estructura de perfiles de Bluetooth y su dependencia.

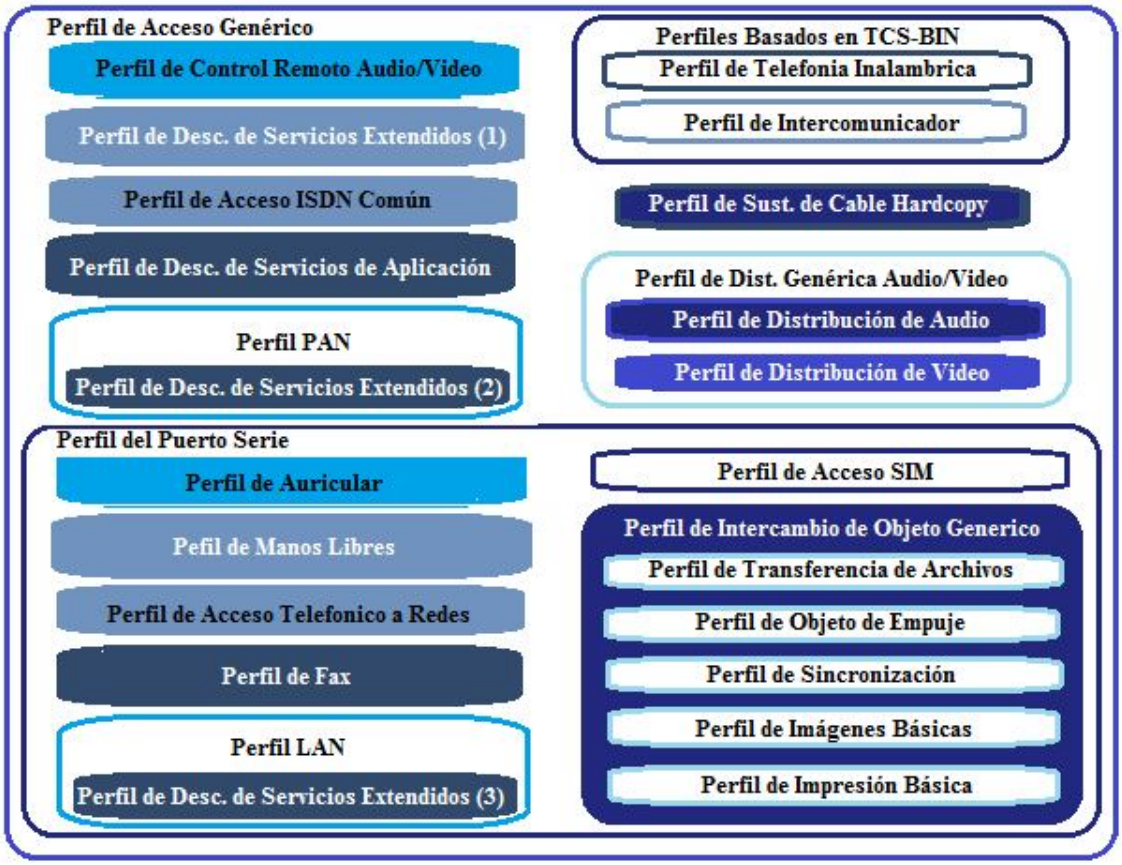

Figura 2.5 Estructura de perfiles Bluetooth.

Los perfiles tienen dependencia de otro perfil si reutilizan partes de él. En el gráfico vemos como el Perfil Sincronización depende del perfil de Intercambio de Objeto Genérico, de Puerto Serie y de Acceso Genérico. Han sido desarrollados más perfiles, y todo indica que se seguirán desarrollando otros nuevos.

2.6.3.1 Acceso Telefónico a Redes (DUN) y Acceso a Redes mediante perfiles PPP (LAN).

El perfil de Acceso Telefónico a Redes (Dial-Up Networking o DUN) se utiliza principalmente con módems y teléfonos celulares. Los escenarios cubiertos por este perfil se describen a continuación:

• Utilización de un teléfono celular por una computadora para simular un modem sin cables que se conecte a un servidor de acceso telefónico a redes o para otros servicios de acceso telefónico relacionados.

• Utilización de un teléfono celular o un modem por un computador para recibir llamadas de datos.

El Acceso a Redes con perfiles PPP (Point to Point Protocol o Protocolo Punto a Punto) (LAN) se puede utilizar en las siguientes situaciones:

- Acceso LAN para un único dispositivo Bluetooth;
- Acceso LAN para múltiples dispositivos Bluetooth;
- Conexión de PC a PC (utilizando emulación de PPP sobre una línea serie).

2.6.3.2. Perfil OBEX Object Push (OPUSH).

OBEX es un protocolo muy utilizado para transferencias de archivos sencillas entre dispositivos móviles. Su uso más importante se produce en comunicaciones por infrarrojos, donde se utiliza para transferencia de ficheros genéricos entre portátiles o dispositivos Palm y para enviar tarjetas de visita o entradas de la agenda entre teléfonos celulares y otros dispositivos con aplicaciones PIM (Personal Information Management o Administración de la Información Personal)

El cliente OBEX se utiliza para introducir y para recuperar objetos del servidor OBEX. Un objeto puede por ejemplo ser una tarjeta de visita o una cita. El cliente OBEX puede obtener un número de canal RFCOMM del dispositivo remoto utilizando SDP. Esto se hace especificando el nombre del servicio en lugar del número de canal RFCOMM. Los nombres de servicios soportados son: IrMC, FTRN y OPUSH. Es posible especificar el canal RFCOMM como un número.

2.7 Principales ataques a Bluetooth

2.7.1 Vulnerabilidades

Como todo estándar de comunicación, Bluetooth también tiene vulnerabilidades que pueden ser explotadas. Estas vulnerabilidades son debidas principalmente a prácticas de codificación erróneas en el desarrollo de los servicios RFCOMM, al desconocimiento de los protocolos de seguridad Bluetooth y a la reutilización de servicios antiguos para protocolos diferentes. Entre las principales vulnerabilidades encontramos las siguientes:

2.7.1.1 Permisos IrMC

- IrMC define los permisos de acceso para los objetos comunes.
- Hay objetos visibles aunque el servicio sea “no emparejado”.
- Servicios abiertos intencionadamente.

2.7.1.2 Errores de pila

- Desbordamiento de Pila.

- Fallos en la implementación de servicios como en el chequeo de la longitud de datos o la integridad de paquetes en OBEX, o terminaciones NULL.

2.7.1.3 Servicios ocultos

- Servicios con los más altos privilegios se dejan abiertos pero escondidos.
- Canales traseros para hacerle la vida más fácil a otros dispositivos.
- Acceso completo al comando AT y por lo tanto a todo el dispositivo.

2.7.2 Comandos AT

Los comandos AT son instrucciones codificadas que conforman un lenguaje de comunicación entre el usuario y un terminal modem.

En un principio, el juego de comandos AT fue desarrollado en 1977 por Dennis Hayes como una interfaz de comunicación con un modem para así poder configurarlo y proporcionarle instrucciones, tales como marcar un número de teléfono. Más adelante, con el avance del baudio, fueron las compañías Microcomm y US Robotics las que siguieron desarrollando y expandiendo el juego de comandos hasta lograr estandarizarlo.
Los comandos AT se denominan así por la abreviatura de attention.

Aunque la finalidad principal de los comandos AT es la comunicación con módems, la telefonía móvil GSM también ha adoptado como estándar este lenguaje para poder comunicarse con sus terminales. De esta forma, todos los teléfonos móviles GSM poseen un juego de comandos AT específico que sirve de interfaz para configurar y proporcionar instrucciones a los terminales. Este juego de instrucciones puede encontrarse en la documentación técnica de los terminales GSM y permite acciones tales como realizar llamadas de datos o de voz, leer y escribir en la agenda de contactos y enviar mensajes SMS, además de muchas otras opciones de configuración del terminal.

Queda claro que la implementación de los comandos AT corre a cuenta del dispositivo GSM y no depende del canal de comunicación a través del cual estos comandos sean enviados, ya sea cable de serie, canal Infrarrojos, Bluetooth, etc. De esta forma, es posible distinguir distintos teléfonos móviles del mercado que permiten la ejecución total del juego de comandos AT o sólo parcialmente.

2.7.3 Ataques de localización y enumeración.

2.7.3.1 Ataques de localización

Las cabeceras Bluetooth no están cifradas, lo que nos permite muchas posibilidades de ataque a la capa Link Manager.
Para perpetrar estos ataques, quienes llevan a cabo estos actos se centran en las capas más altas de la pila de protocolos y sacan ventaja de ellas permitiéndoles entre otras cosas:

- Localizar dispositivos Bluetooth en modo “visible”.
- Localizar dispositivos Bluetooth en modo “no visible”.
- Enumerar información de sus servicios

2.7.3.2 Ataques de enumeración de servicios.

Ahora ya tengo localizados todos los dispositivos Bluetooth con los que podemos “contactar”, y seremos capaces de averiguar lo siguiente:

- La dirección Bluetooth (por ejemplo MAC).
- Clase de dispositivo.
- Tipo de dispositivo.
- Nombre del dispositivo.

Para la extracción de toda esta información se necesita seguir una serie de pasos, por los que se ira ascendiendo a través de la pila de protocolos, desde el HCI (nivel Link) hasta el SDP (aplicación), para ir recogiendo la información.

Una vez vista toda la teoría referente a la estructura del protocolo Bluetooth y, habiéndo centrado en lo relativo a la Seguridad, a continuación se procede a documentar algunas técnicas, herramientas y aplicaciones basadas en la ejecución de comandos AT que permiten llevar a la práctica aspectos de la Inseguridad en Bluetooth.

Estos ataques crean una conexión al dispositivo, dando acceso al juego de comandos AT, los cuáles nos permiten, básicamente, las siguientes posibilidades:

- Control de las llamadas.
- Mandar/leer/borrar SMS.
- Leer/grabar/eliminar entradas de la agenda.
- Desviar/realizar llamadas de voz/datos.

Por ejemplo, se podrian espiar las conversaciones mantenidas en una reunión haciendo que el teléfono de la víctima realice una llamada silenciosa a nuestro teléfono o a otro teléfono de cualquier parte del mundo. De esta forma, se crea un canal de comunicación vía GSM que permitirá escuchar toda la conversación de la reunión.

También se podría instalar una pasarela en el teléfono de la víctima, redirigiendo sus llamadas a algún teléfono, teniendo así la posibilidad de escuchar y grabar sus conversaciones sin su conocimiento. O se podría mandar un SMS a través de su teléfono, haciéndole creer al destinatario que lo mandó la víctima. Es posible incluso hacer que el mensaje no se quede almacenado en la memoria de la víctima.

Todo esto es debido a que la implementación de los mecanismos de seguridad suele ser muy pobre. Además se cuenta con varios servicios no documentados o abiertos en los canales RFCOMM.

2.8 Seguridad y corrección de errores en Bluetooth

Como ya se ha visto la seguridad en una red informática es básica para su buen desempeño y para proteger la información que fluye en la misma. Las redes Bluetooth cuentan con ciertas características que ayudan a proteger la información y mejorar el nivel de servicio de la red.

2.8.1 Modos de seguridad.

Hay tres modos primarios de seguridad:

***Modo 1. Sin seguridad*.** Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además el dispositivo se sitúa en modo "promiscuo", permitiendo que todos los dispositivos Bluetooth se conecten a él.

Modo 2. En la capa L2CAP, nivel de servicios. Los procedimientos de seguridad son inicializados después de establecerse un canal entre el nivel LM y el de L2CAP. Un gestor de seguridad controla el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos de seguridad que operen en paralelo.
Su interface es muy simple y no hay ninguna codificación adicional de PIN o claves.

Modo 3. En el nivel de Link. Todas las rutinas están dentro del chip Bluetooth y nada es transmitido en plano. Los procedimientos de seguridad son iniciados antes de establecer algún canal. Aparte del cifrado, tiene autenticación PIN y seguridad MAC. Su metodología consiste en compartir una clave de enlace secreta entre un par de dispositivos. Para generar esta clave, se usa un procedimiento de "pairing" (emparejamiento) cuando los dos dispositivos se comunican por primera vez.

2.8.2 Emparejamiento de Dispositivos

Por defecto, la comunicación Bluetooth no se valida, por lo que cualquier dispositivo puede en principio hablar con cualquier otro. Un dispositivo Bluetooth (por ejemplo un teléfono celular) puede solicitar autenticación para realizar un determinado servicio (por ejemplo para el servicio de marcación por modem).

La autenticación de Bluetooth normalmente se realiza utilizando códigos PIN. Un código PIN es una cadena ASCII de hasta 16 caracteres de longitud. Los usuarios deben introducir el mismo código PIN en ambos dispositivos.

Una vez que el usuario ha introducido el PIN adecuado ambos dispositivos generan una clave de enlace. Una vez generada, la clave se puede almacenar en el propio dispositivo o en un dispositivo de almacenamiento externo. La siguiente vez que se comuniquen ambos dispositivos se reutilizará la misma clave.

Es importante recordar que si la clave de enlace se pierde en alguno de los dispositivos involucrados se debe volver a ejecutar el procedimiento de emparejamiento.
No existe ninguna limitación en los códigos PIN a excepción de su longitud. Algunos dispositivos (por ejemplo los dispositivos de mano Bluetooth) pueden obligar a escribir un número predeterminado de caracteres para el código PIN.

2.8.3 Inicialización y Generación de la claves

La Clave de Linkado es generada durante una fase de inicialización, cuando dos dispositivos empiezan a comunicarse. Según la especificación Bluetooth, la clave es generada durante la fase de inicialización cuando el usuario introduce un PIN idéntico en ambos dispositivos. Después de completarse la inicialización, los dispositivos se autentican de manera automática y transparente y se lleva a cabo el cifrado de la conexión.

Generación de claves en la Inicialización: En la figura 2.6 se muestran en un esquema los algoritmos E21 y E22 son agrupados en uno genérico llamado E2.

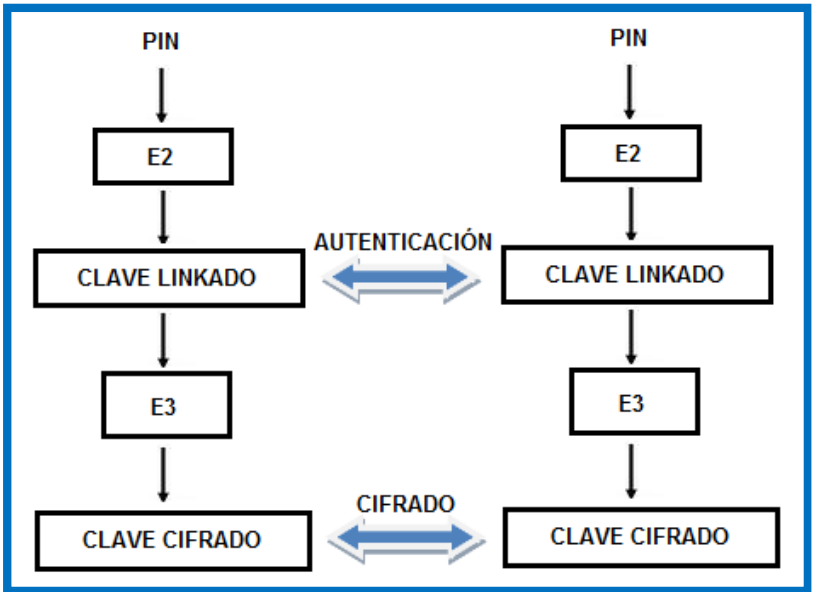

Figura 2.6 Generación de claves de inicialización.

El proceso de Inicialización se desarrolla según los siguientes pasos:

2.8.3.1 Generación de una clave de inicialización (K init).

Aplicando el *PIN* del dispositivo y su longitud, el *BD_ADDR* (48 bits) y un número aleatorio de 128bits, *IN_RAND* al algoritmo E22.

El resultado es una palabra de 128 bits, referida como K init.
Resaltamos que el PIN está disponible en ambos dispositivos Bluetooth, y que IN_RAND es transmitido en plano.

Respecto a BD_ADDR, si uno de los dispositivos tiene un PIN fijo, se usa la BD_ADDR del dispositivo asociado, y si ambos tienen un PIN variable, se usa el PIN del dispositivo que recibe el IN_RAND (el esclavo).

Esto debido a que algunos dispositivos tienen un PIN predefinido que no puede ser modificado, con lo cual este PIN tiene que introducirse en el dispositivo al que queremos emparejarnos. Si ambos tienen un PIN fijo, no pueden emparejarse. La figura 2.7 muestra un esquema de cómo se genera la clave de inicialización (K init).

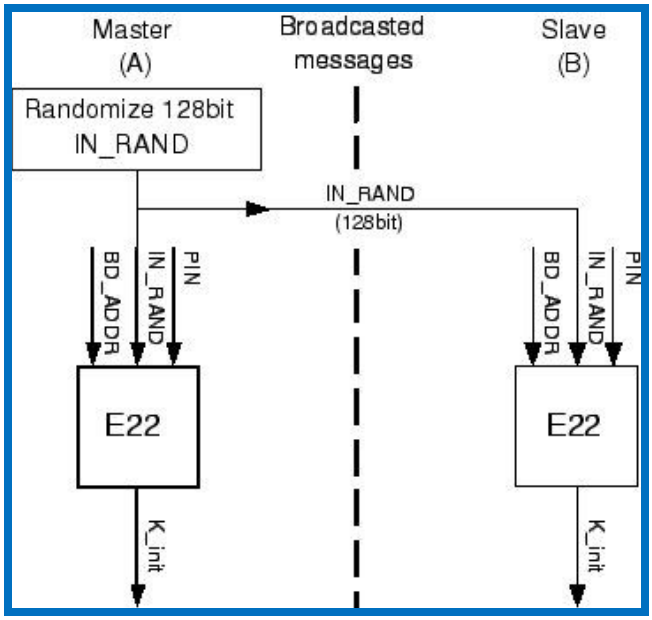

Figura 2.7 Generación de una clave de inicialización (K init).

2.8.3.2 Generación de la clave de enlace K ab.

Usando el algoritmo E21, ambos dispositivos crean la clave de enlace.

Los dispositivos usan la clave de inicialización para intercambiar dos nuevos números aleatorios de 128 bits, conocidos como LK_RAND A y LK_RAND B. Cada dispositivo genera un número aleatorio de 128 bits y lo envía al otro dispositivo previamente sometidos al cifrado XOR bit a bit con K init. Dado que ambos dispositivos conocen K init, cada dispositivo conoce ambas LK_RAND.

Usando como parámetros de entrada un BD_ADDR y el LK_RAND, el algoritmo E21 obtiene la clave de enlace K ab. La figura 2.8 muestra la manera cómo se genera la clave de enlace K ab.

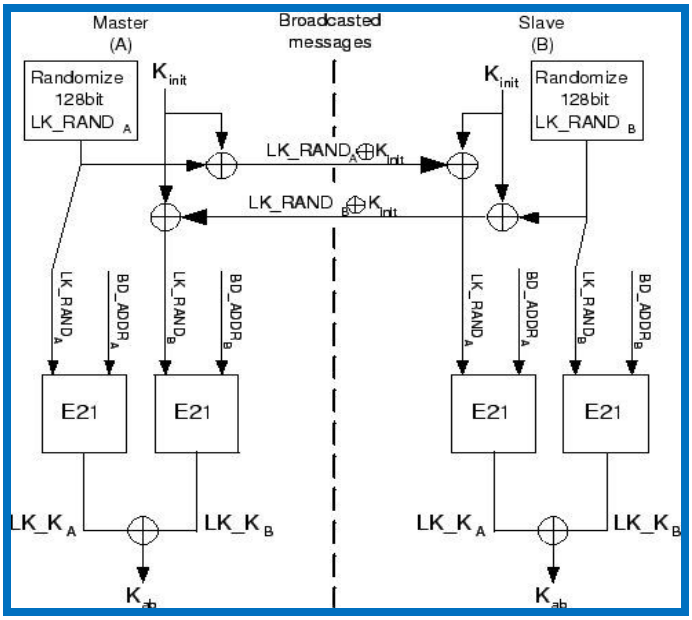

Figura 2.8 Generación de la clave de enlace K ab.

2.8.3.3 Autenticación Bluetooth

El procedimiento de autenticación sigue el conocido esquema "challenge-response", reto-respuesta.
Los pasos son los siguientes:

• El "demandante" transfiere su dirección de 48 bits (BD_ADDR) al "verificador".

• El verificador le transfiere un "desafío" aleatorio de 128 bits (AU_RAND) al demandante.

• El verificador usa el algoritmo E1 para generar el "response" de autenticación, usando como parámetros la dirección del demandante, BD_ADDR b, la Clave de enlace, K ab, y el desafío. El demandante realiza la misma operación.

• El demandante le devuelve el "response", SRES, al verificador.

• El verificador compara el SRES del demandante con el que el ha calculado.

• Si los valores de los 32 bits de los SRES son idénticos, el verificador establece la conexión.

La figura 2.9 ilustra el método de autenticación empleado por Bluetooth.

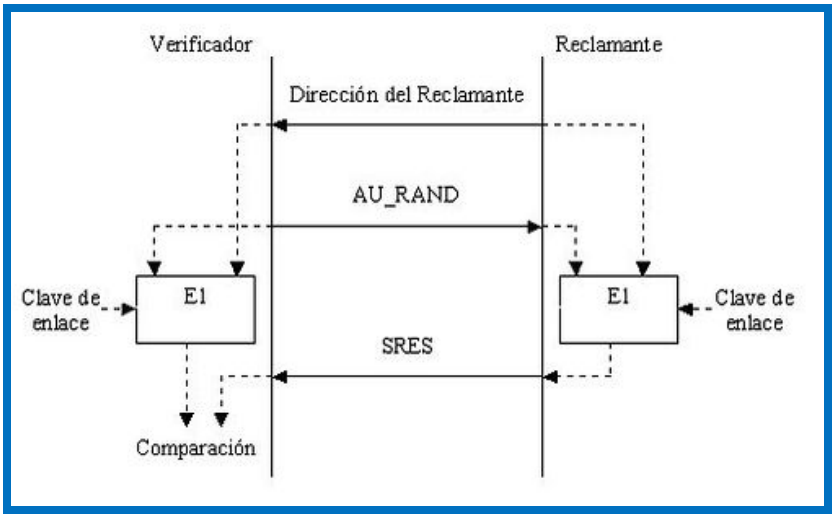

Figura 2.9 Método de autenticación Bluetooth.

En este proceso, se crea además un número de 96 bits llamado ACO (Authenticated Ciphering Offset) en ambos dispositivos, que será usado para la creación de la Clave de Cifrado.

2.8.3.4 Generación de la clave de cifrado

Cuando el Link Manager (LM) activa el cifrado, se crea la Clave de Cifrado, K c , que es modificada cada vez que el dispositivo entra en dicho modo.

La Clave de Cifrado es generada aplicando al algoritmo E3 la Clave de Enlace, un número aleatorio de 128 bits y un Ciphering Offset (COF) basado en el valor de ACO del proceso de autenticación. (Ver figura 2.10).

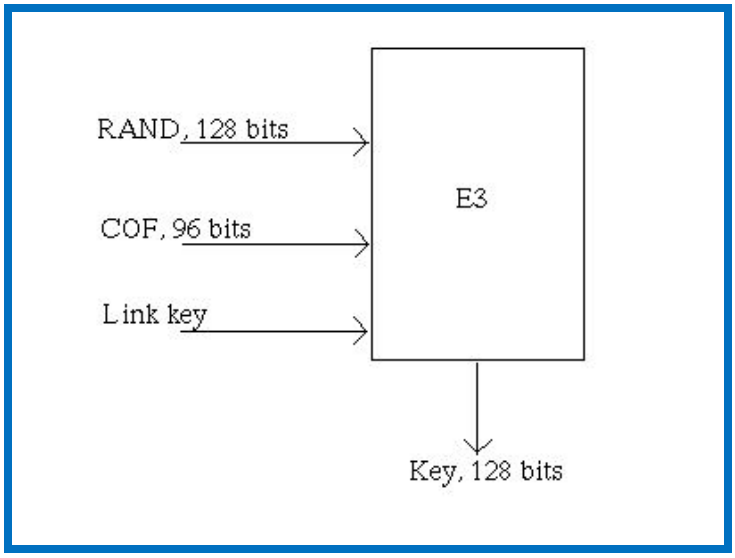

Figura 2.10 Generación de la clave de cifrado.

En este punto ya estaríamos en condiciones de transferir datos cifrados.

2.8.4 Proceso de cifrado en Bluetooth.

La especificación de Bluetooth permite tres modos de cifrado diferentes.

• Modo 1. Ninguna parte del tráfico de datos es cifrada.

• Modo 2. El tráfico general va sin cifrar, pero el tráfico dirigido individualmente se cifra según las claves individuales de la conexión.

• Modo 3. Todo el tráfico es cifrado acorde a la Clave de Cifrado.

La información de usuario es protegida por cifrado de la carga útil (payload), ya que el código de acceso y la cabecera del paquete nunca son cifrados. El cifrado se lleva a cabo con el algoritmo de cifrado E0, que consiste básicamente de tres partes, como se ve en la figura 2.11:

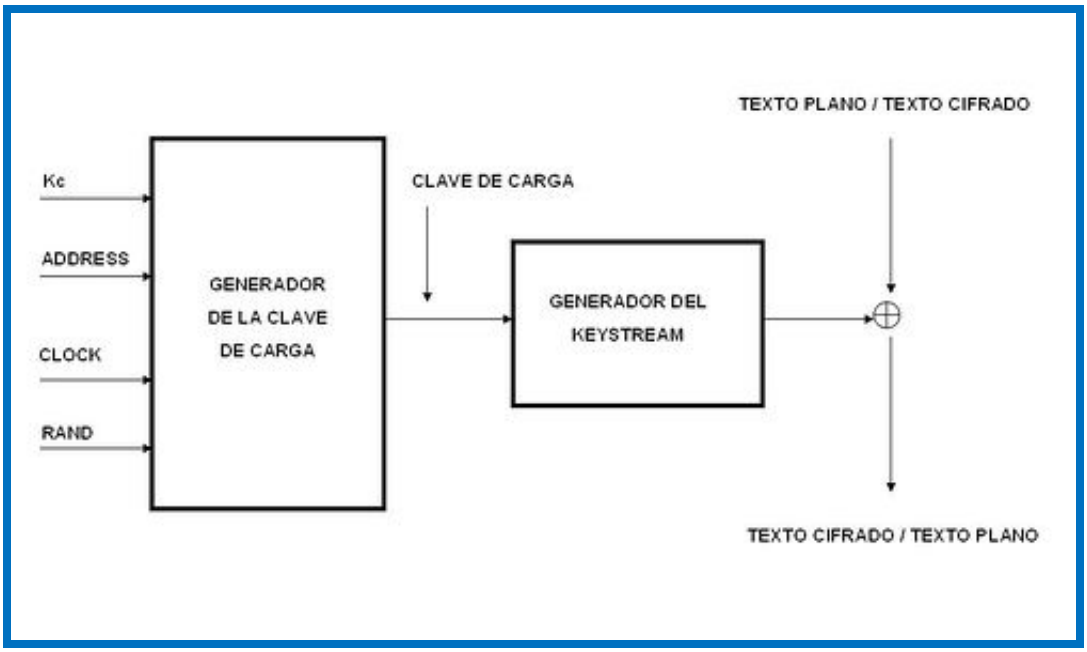

Figura 2.11 Algoritmo de cifrado Bluetooth.

Una parte que realiza la inicialización (generación de la clave de carga útil). Una segunda parte que es el generador de cadenas de claves, y finalmente una tercera parte en la cual se realiza el cifrado o el descifrado.

Los parámetros de entrada a dicho algoritmo serán la clave de cifrado que se obtiene del algoritmo E3, la BD_ADDR del maestro y el reloj del mismo y un número aleatorio.
El Generador de Clave de Key Stream combina los bits de entrada de una forma apropiada y los guarda en 4 registros de desplazamiento retroalimentados, conocidos como Linear

Feedback Shift Registers (LSFR). Estos registros son de 25, 31, 33 y 39 bits (128 en total). Este método viene derivado del generador de cifrado de Streams de Massey y Rueppel. Cuando el cifrado está activo, el maestro envía un número aleatorio (RAND) al esclavo. Antes de la transmisión de cada paquete, el LFSR se inicializa en el Generador de Clave de Carga mediante la combinación de RAND, la identificación del maestro, la clave de cifrado K c y el número de reloj (o número de Slot).

Como el tamaño de la Clave de Cifrado varía desde 8 a 128 bits, tiene que ser "negociado" entre los dispositivos previamente. En cada dispositivo hay un parámetro que define la longitud máxima permitida de la clave. En esta negociación, el maestro manda su sugerencia al esclavo, y este puede aceptarla o enviar otra sugerencia. Así hasta que haya consenso entre los dispositivos, o la uno de ellos aborte la negociación.

En cada aplicación, hay definido un tamaño mínimo de clave aceptable, y si estos requerimientos no son cumplidos por ambos dispositivos, la aplicación aborta la negociación, y el cifrado no puede ser usado. Esto es necesario para evitar la situación donde uno de los dispositivos fuerce un cifrado débil algún fin malicioso.

Finalmente se genera el Key Stream (K cipher) que es sumada en módulo-2 (operaciones sobre números binarios que desperdician o no tienen en cuenta las unidades que se deben llevar al siguiente nivel) a los datos que se desean cifrar. El descifrado se realizará exactamente de la misma manera usando la misma clave que se usó para el cifrado.

Cada paquete de carga útil es cifrado separadamente, lo cual se consigue si tenemos en cuenta que una de las entradas al algoritmo E0 es el reloj del maestro, el cual cambia una unidad cada intervalo de tiempo (625µs), por lo que la clave de carga útil será diferente para cada paquete, excepto para aquellos que ocupen más de un intervalo de tiempo, en cuyo caso el valor del reloj del primer intervalo de tiempo del paquete será el que se utilizará para todo el paquete. (Ver figura 2.12).

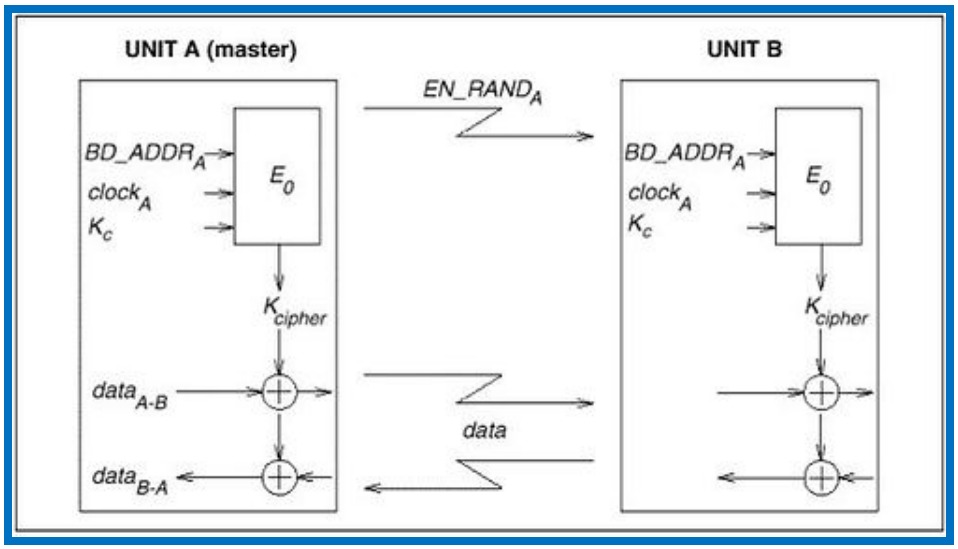

Figura 2.12 Descripción funcional del procedimiento de cifrado.

2.8.5 Debilidades de la seguridad.

2.8.5.1 Generales

• No está demostrada la fuerza del generador pseudo aleatorio del procedimiento "challenge-response". Se podrían producir números estáticos o repeticiones periódicas que redujeran su efectividad.

• Los PINs cortos son permitidos. De hecho se puede elegir la longitud del PIN, que va de entre 1 a 16 bytes. Normalmente los usuarios los prefieren muy cortos.

• No hay una forma "adecuada" de generar y distribuir el PIN. Establecer PINs en una red Bluetooth grande y con muchos usuarios puede ser difícil, y esto lleva normalmente a problemas de seguridad.

• La longitud de la clave de cifrado es negociable. Es necesario un procedimiento de generación de claves más fuerte.

• En el caso del modo 3, la clave maestra es compartida. Es necesario desarrollar un esquema de transmisión de claves mejorado.

• No existe autenticación de usuarios. Sólo está implementada la autenticación de dispositivos.

• No hay límite de intentos de autenticación.

• La autenticación es un simple "challenge-response" con hashes. Según esta diseñado, el esquema es vulnerable a ataques "Man in the Middle".

• Los servicios de seguridad son limitados. Servicios de auditoría, de no repudio, etc., no están implementados.

2.8.5.2 Vulnerabilidades del cifrado.

Dejando aparte de que el cifrado es opcional, podemos darnos cuenta de que también padece de varias vulnerabilidades:

• El algoritmo de cifrado por bloques E0 es débil. Aunque se perfilaba como relativamente seguro hace pocos años. Su sistema de creación del Stream para el cifrado es mucho más complejo, y soluciona los problemas de reutilización de claves como el que tiene el RC4 del Wi-Fi (802.11b).

Sin embargo, como con todos los algoritmos de cifrado, su seguridad va disminuyendo de manera gradual.

Aunque E0 permite longitudes de clave que van desde 1 hasta 16 bytes (8-128 bits),

Jakobbson y Wetzel presentaron un ataque con complejidad matemática de O (2^{100}) (esto es el equivalente a reducir la longitud de clave efectiva de 128 a 100 bits).

• Uso parcial del reloj. Como hemos visto, el reloj del dispositivo maestro es un parámetro de entrada para la generación del Stream de cifrado. Aunque parece que por un fallo de diseño el bit más significativo de su valor es ignorado, permitiendo este hecho entre otras cosas ataques tipo Man in The Middle.

• Los datos cifrados pueden ser manipulados. Incluso con el cifrado más fuerte, las características de los cifrados de Stream permiten que los datos interceptados en un ataque Man in The Middle puedan ser convenientemente manipulados dependiendo de la cantidad de texto cifrado conocida. Así es posible por ejemplo manipular cabeceras IP.

2.9 Usos y aplicaciones

El estándar Bluetooth puede ser utilizado en un gran número de aplicaciones y/o dispositivos de comunicación, entre los principales usos y aplicaciones encontramos los siguientes:

Lista de aplicaciones

- Conexión sin cables entre los celulares y PDA´s.
- Equipos de manos libres y
- Dispositivos inalámbricos para vehículos.
- Red inalámbrica en espacios reducidos donde no sea tan importante un ancho de banda grande.
- Comunicación sin cables entre la computadora y dispositivos de entrada y salida. Principalmente impresoras, teclado y mouse.
- Transferencia de ficheros entre dispositivos vía OBEX.
- Transferencia de fichas de contactos, citas y recordatorios entre dispositivos vía OBEX.
- Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.
- Controles remotos (tradicionalmente dominado por el infrarrojo). Enviar pequeñas publicidades desde anunciantes a dispositivos con Bluetooth. Un negocio podría enviar publicidad a teléfonos móviles cuyo Bluetooth (los que lo posean) estuviera activado al pasar cerca.
- Consolas para video juegos, lo que les permite utilizar mandos inalámbricos

En la figura 2.13 se ilustran los principales usos y aplicaciones Bluetooth.

Figura 2.13 Usos y aplicaciones Bluetooth

2.10 Futuro de Bluetooth

Con el paso del tiempo y con la demanda para mejorar esta tecnología, se han implementado correcciones y mejoras para crear una versión de la tecnología Bluetooth con opción a grandes anchos de banda. Esta nueva versión permitirá alcanzar los requisitos de sincronización y transferencia de grandes cantidades de datos así como de contenidos de alta definición para dispositivos portátiles, proyectores multimedia, televisores y teléfonos VOIP.

Al mismo tiempo, la tecnología Bluetooth continuará satisfaciendo las necesidades de aplicaciones de muy bajo consumo como ratones, teclados o auriculares permitiendo a los dispositivos seleccionar la capa física más apropiada para sus requisitos.

La tecnología Bluetooth lucha por imponerse en las computadoras y sus periféricos como modo estándar de conexión. Ahora, las nuevas funcionalidades de los móviles de última generación han convertido el Bluetooth en una tecnología con potencial para conectar una amplia gama de dispositivos y periféricos de la computadora. En la actualidad, numerosos dispositivos y periféricos se basan en la tecnología Bluetooth, desde los clásicos manos libres y auriculares más básicos, hasta altavoces en forma de pulseras, pensados para utilizar en vehículos.

A pesar de integrarse por defecto en las computadoras actuales, el estándar Bluetooth no es compatible con muchos de los periféricos disponibles en el mercado. Aunque fabricantes como Microsoft o Logitech tienen aparatos que usan esta tecnología, optan por utilizar sus propios transmisores propietarios inalámbricos en dispositivos como ratones de computadora. Por su parte, Apple es uno de los fabricantes de ordenadores que más apuesta

por el Bluetooth como tecnología inalámbrica para la conexión de teclados, ratones y su trackpad multitáctil denominado Magic Trackpad.

Esta tecnología no sólo está presente en periféricos, sino que también se ha implantado en dispositivos para el hogar, en respuesta a las peticiones de los usuarios para no utilizar cables.

Bluetooth es una de las muchas tecnologías que utilizamos a lo largo del día y la posibilidad de conectividad inalámbrica y la compatibilidad con muchos dispositivos y funciones hacen de la misma una solución completa para casi todo. Bluetooth SIG pretende implementar mejoras en el estándar y así lograr integrar dispositivos que hasta el momento eran impensables por el consumo.

Todas éstas permitirán que muchos dispositivos puedan beneficiarse de la conectividad Bluetooth, algo hasta el momento impensable debido al alto consumo energético y a ciertos posibles riesgos de seguridad. Estamos hablando de mercados como salud, deporte, seguridad y entretenimiento.