ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA ELECTRONICA EN TELECOMUNICACIONES

ANÁLISIS DE LAS VULNERABILIDADES DE LA TECNOLOGÍA BLUETOOTH REFERENTE A LA SEGURIDAD

TONY ROBERT ANGULO ACUNSO

Sangolquí – Ecuador

2009

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado "ANÁLISIS DE LAS VULNERABILIDADES DE LA TECNOLOGÍA BLUETOOTH REFERENTE A LA SEGURIDAD", ha sido desarrollado en su totalidad por el Sr. Tony Robert Angulo Acunso con C.I. 080250643-6, como previo requisito para la obtención del título de Ingeniero Electrónico, bajo nuestra dirección.

_____	_____
Ing. Gonzalo Olmedo	Ing. Carlos Romero
DIRECTOR	CODIRECTOR

RESUMEN

El presente trabajo analiza los tipos de seguridades que presenta la tecnología Bluetooth, donde se realizar un estudio que permite establecer los protocolos que ofrecen seguridad para tener una comunicación sin interferencia de otros dispositivos que puedan irrumpir y ocasionar la perdida de paquetes de información, sobre la formulación de un nuevo protocolo el cual se obtendrá mediante el análisis de los diferentes tipos de seguridad que tiene la tecnología bluetooth y las redes inalámbricas, y la simulación de una red Bluetooth en la que podremos observar la potencia, señal a ruido y la velocidad con la cual son transferidos los paquetes y ver como es el desempeño de esta tecnología y conjuntamente con los protocolos ya existentes formular el nuevo protocolo que nos brinde mayor seguridad en el momento de realizar alguna transferencia de información o conectarnos a alguna red que esté a nuestro alcance.

Esta simulación la realizaremos mediante la utilización del software Network Simulator, ya que este simulador es una potente herramienta de simulación de redes, nos ayuda mucho en el momento de analizar los resultados, ya que permite obtener conclusiones que nos ayuden a la realización de la Tesis.

DEDICATORIA

Dedico este trabajo a mis Padres Maricela Acunso y a Tony Angulo ya que con su infinito cariño, apoyo y comprensión me han ayudado a salir adelante para convertirme en una persona de bien.

AGRADECIMIENTO

Agradezco a Dios por haberme dado la sabiduría para escoger la carrera de Telecomunicaciones, agradezco a mis Hermanos, Amigos, Profesores y a toda mi Familia que han estado allí para darme su aliento en situaciones difíciles haciendo posible que Yo logre obtener el título que con tanto anhelo he esperado.

PRÓLOGO

Bluetooth se ha convertido en el estándar de referencia de comunicaciones inalámbricas para redes de área personal que permite la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. En un entorno que cada día exige una mayor interoperabilidad entre los diferentes equipos que existen en el mercado, la popularidad de Bluetooth se ha visto fuertemente impulsada por su integración en dispositivos de la vida cotidiana como teléfonos móviles y por facilitar la interconexión inalámbrica de periféricos a un ordenador. Así mismo, han surgido modelos de uso de la tecnología Bluetooth que hacen habitual el empleo de dispositivos de última generación, como los equipos manos libres de automóvil y auriculares, que permiten mantener conversaciones telefónicas con absoluta libertad mientras se conduce un vehículo o se trabaja en la oficina. Es importante destacar que Bluetooth es un protocolo de comunicaciones seguro y robusto, y que las fallas de seguridad descubiertas se deben a la incorrecta implementación de los mecanismos de seguridad de Bluetooth en los dispositivos por parte de los fabricantes. La publicación de estas vulnerabilidades ha hecho reaccionar a los fabricantes de dispositivos Bluetooth, obligándoles a mejorar la seguridad en sus equipos antes de su lanzamiento en el mercado.

No obstante, el estudio continúa y actualmente se siguen publicando nuevas vulnerabilidades y herramientas que permiten su explotación.

Por tal motivo, es evidente la necesidad de efectuar un análisis de las vulnerabilidades que permita comprender las fallas de estos protocolos, llegando a un estudio que nos permita plantear un nuevo protocolo que brinde una mayor seguridad en los dispositivos que usan esta tecnología de comunicación inalámbrica Bluetooth.

ÍNDICE DE CONTENIDO

CAPÍTULO I:
INTRODUCCIÓN AL BLUETOOTH

CAPÍTULO II:
PROTOCOLOS DE SEGURIDAD

CAPÍTULO III:

SIMULACION DE UNA RED BLUETOOTH

CAPÍTULO IV:

PROPUESTA DE UN PROTOCOLO DE SEGURIDAD

CAPÍTULO V:

ÍNDICE DE TABLAS

CAPÍTULO I

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

GLOSARIO DE TERMINOS

SIG.- Special Interest Group, grupo de interés especial

ISM.- Industrial, Scientific and Medical

FHSS.- Frequency Hopping Spread Spectrun

GFSK.- Gaussian Frequency Shift Keying

LAP.- Low Address Part

CAC.- Código de acceso al canal

DAC.- Código de acceso al dispositivo

IAC.- Código de acceso de búsqueda o indagación

GIAC.- IAC general

DIAC.- IAC dedicado

SCO.-Synchronous

ACL.- Asynchronous connectionless

DSP.- Digital signal processor

ARQ.- Automatic repeat request

FEC.- Forward error correction

LMP.- Link manager protocol

BD_ADDR.- Bluetooth device address

AM_ADDR.- Active member address

PM_ADDR.- Parked member address

AR_ADDR.- Access request address

HCI.- Host controller interface

AMF.- Adaptive frequency hopping

EDR.- Enhenced data rate

GAP.- Perfil de acceso genérico

SPP.- Perfil de puerto serie

SDAP.- Perfil de aplicación de descubrimiento de servicio

GOEP.- Perfil generic de intercambio de objetos

SDP.- Protocolo de descubrimiento de servicio

CTP.- Perfil de telefonía inalámbrica

IP.- Perfil de intercomunicaciones

DUN.- Perfil de acceso telefónico a redes

HS.- Perfil de auriculares

FP.- Perfil de fax

LAP.- Perfil de acceso a red

FTP.- Perfil de transferencia de archivos

RFCOMM.- Radio Frequency Communication

IrDA.- Infrared Data Association

IETF.- Internet Engineering Task Force

ACL.- Access Control List

OSA.- Open System Authentication

WEP.- Wired Equivalent Protocol

WAP.- Protocolo de Aplicación Inalámbrica

CNAC.- Closed Network Access Control

NAM.- Network animator

CAPÍTULO I

INTRODUCCIÓN AL BLUETOOTH

1.1. Definición del Bluetooth

Bluetooth es una tecnología que permite conectar dispositivos electrónicos entre sí de forma inalámbrica, es decir, sin cables (wireless). Por lo tanto pueden conectarse computadoras de escritorio o portátiles, celulares, PDAs (entre otros dispositivos) entre sí.

Esta tecnología utiliza ondas de radio de corto alcance de 2,4 a 2,48 GHz de frecuencia, alcanzando distancias de hasta 10 metros, incluso atravesando objetos o paredes. Es posible llegar hasta los 100 metros de conexión, pero con un aumento considerable en el gasto de baterías. Al ser la conexión inalámbrica, evitamos los cables entre los dispositivos. Es posible intercambiar todo tipo de datos con cualquier dispositivo que disponga del software y el hardware necesarios para hacer funcionar el bluetooth [1].

1.2. Descripción del Bluetooth

Bluetooth es la especificación que define un estándar global de comunicaciones inalámbricas para redes de área personal que permite la transmisión de voz y datos entre diferentes equipos mediante un enlace de radiofrecuencia en entornos de comunicaciones móviles y estáticos.

La tecnología Bluetooth se basa en los siguientes aspectos:

- El sistema deberá ser universal, es decir, operar en todo el mundo.
- El sistema será capaz de establecer comunicación entre dos dispositivos que cumplan con las especificaciones bluetooth, cualquiera que sea su naturaleza: PC, teléfono móvil, accesorios de automóvil, etc.
- El emisor de radio deberá consumir poca energía, ya que debe integrarse en equipos alimentados por baterías.
- Se tratara de un sistema basado en un protocolo robusto y seguro [2].

1.2.1. Etimología del Bluetooth

El rey vikingo Harald II Blåtand, que reinó en Dinamarca entre los años 940 y 986, nunca podría haberse imaginado que su persona y su sobrenombre en inglés, Bluetooth, iban a ponerse de moda a finales del siglo XX y a principios del siglo XXI, para dar nombre a un estándar de comunicación inalámbrica que promete revolucionar el mundo de las comunicaciones y de la informática.

Su nombre, Blåtand, está formado por dos palabras del antiguo danés: *blå,* que significa 'hombre de piel oscura', y *tand,* 'hombre fuerte'. A pesar de esta etimología es más conocido por su apodo en inglés, *Bluetooth*, quizás por mera adaptación o deformación fonética, ya que el hecho de que tuviera un diente azul no llega a ser ni tan siquiera leyenda. Tampoco daba Harald el prototipo del vikingo en cuanto a su físico, su nombre ya nos dice que era moreno y no rubio, pero ocupó un lugar importante en la historia de su país al unificar dos países próximos pero separados por un mar, Dinamarca y Noruega, uniéndolos además bajo una sola fé, el cristianismo.

Estas circunstancias hicieron que la compañía escandinava Ericsson, desarrolladora de un estándar para las comunicaciones inalámbricas entre dispositivos de distinta naturaleza (computadoras, teléfonos móviles, agendas electrónicas y otros periféricos) bautizara al nuevo y prometedor estándar precisamente como Bluetooth. La elección de este nombre, aparte de la simbología que conlleva el personaje, introduce además en el juego el color

azul, tan unido a la propia firma Ericsson y a algunas de sus colaboradoras (IBM, NOKIA...) cuando no a la propia tecnología, llamada también el *sector azul.*

Bluetooth (Diente Azul, como también ha empezado a denominarse en español), al igual que su antecesor vikingo, conecta mundos diferentes y físicamente separados bajo una sola fe, el propio estándar en este caso, para crear lo que se ha dado en llamar "Redes de Área Personal", que incorporan en un radio de corta distancia los artilugios compañeros habituales de los activos hombres de negocios: el móvil, la agenda electrónica, la computadora portátil, así como otro tipo de periféricos más propios de la oficina: impresoras, terminales de fax, escáneres, etc [3].

El logo de Bluetooth combina la representación de las runas nórdicas Hagalaz (transcrito por 'H') y Berkana (transcrito por 'B') en un mismo símbolo [4]:

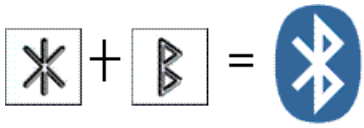


Figura 1.1 Logo del Bluetooth

1.2.2. Historia del Bluetooth

En 1994, Ericsson Mobile Communications, la compañía global de telecomunicaciones con base en Suecia, comenzó un estudio de viabilidad de una interfaz de radio de baja potencia y bajo coste entre teléfonos móviles y otros accesorios, con el objetivo de eliminar los cables. El estudio era parte de un proyecto más amplio que investigaba cómo conectar diferentes dispositivos de comunicaciones a la red celular a través de un teléfono móvil. La compañía determinó que el último enlace en ese tipo de conexión debería ser un enlace de radio de corto alcance. A medida que progresaba el proyecto, se hizo evidente que este tipo de enlace de radio de corto alcance podía ser utilizado ampliamente en un gran número de aplicaciones.

El trabajo de Ericsson en esta área atrajo la atención de IBM, Intel, Nokia y Toshiba. Estas compañías decidieron formar en febrero de 1998 un grupo especial de investigación denominado ***SIG*** *(Special Interest Group) Bluetooth*, con el objetivo de desarrollar, promover, definir y publicar las especificaciones de esta tecnología inalámbrica de corta distancia [2].

1.3. SIG de Bluetooth

En 1998, Ericsson, IBM, Intel, Toshiba y Nokia formaron un consorcio y adoptaron Bluetooth como nombre para su especificación. En diciembre de 1999, 3Com, Lucent, Microsoft y Motorola se unieron a dicho grupo como promotores del Bluetooth SIG (Special Interest Group, grupo de interés especial). Posteriormente Lucent transfirió su participación a su satélite Agere Systems y 3Com abandonó el grupo de promotores. Posteriormente Agere Systems se fusionó con la LSI Corporation y abandonó el grupo en agosto de 2007.

El Bluetooth SIG es una asociación privada sin ánimo de lucro con sede en Bellevue, Washington. A la fecha de septiembre de 2007, el SIG está formado por más de 9000 compañías de telecomunicaciones, informática, automovilismo, música, textil, automatización industrial y tecnologías de red. Tiene pequeños grupos de personal dedicado al grupo en Hong Kong, Suecia y Estados Unidos. Los miembros del SIG dirigen el desarrollo de la tecnología inalámbrica Bluetooth, además de implementar y comercializar la tecnología en sus productos. El Bluetooth SIG por sí mismo no fabrica ni vende dispositivos Bluetooth [5].

Figura 1.2 Algunos Integrantes del SIG [6]

1.4. Descripción de la tecnología Bluetooth

Bluetooth incorpora las siguientes especificaciones técnicas:

La frecuencia de radio con la que trabaja se sitúa en el rango de 2.4 a 2.48 GHz de la banda ISM (Industrial, Scientific and Medical) disponible a nivel mundial y que no requiere licencia de operador, lo que significa una compatibilidad universal entre dispositivos Bluetooth. Con el fin de evitar interferencias con otros protocolos que operen en la misma banda de frecuencias, Bluetooth emplea la técnica de salto de frecuencias ***(FHSS, Frequency Hopping Spread Spectrum)***, que consiste en dividir la banda en 79 canales de longitud 1 MHz y realizar 1600 saltos por segundo [2].

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.

clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Rango (m)
clase 1	100	20	100
clase 2	2,5	4	10
clase 3	1	0	0,1

Tabla 1.1 Clases de dispositivos 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 [7].

1.5. Topología de red Bluetooth

A diferencia de otras tecnologías LAN inalámbricas, como IEEE 802.11 (Wi-Fi), diseñadas para dispositivos que se hallen dentro o en los alrededores de un mismo edificio,

los dispositivos que utilicen las redes PAN inalámbricas IEEE 802.15, incluyendo Bluetooth, podrán comunicarse en cualquier parte del mundo de forma stand-alone, incluso a bordo de un barco o avión y sin necesidad de utilizar equipo hardware adicional, como puntos de acceso.

Cuando un dispositivo Bluetooth está dentro del radio de cobertura de otro, pueden establecer un enlace entre ellos. Hasta ocho unidades Bluetooth pueden comunicarse entre ellas y formar lo que se denomina una ***Picone***t o ***Picorred***. La unión de varias Piconets se denomina ***Scatternet*** o ***Red Dispersa***.

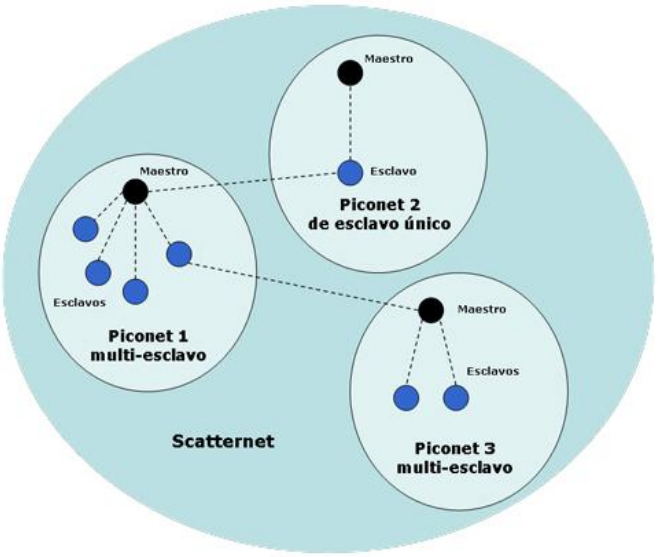


Figura 1.3 Red dispersa o Scatternet

Los dispositivos dentro de una piconet juegan dos papeles: maestro o esclavo. En todas las piconets sólo puede haber una unidad maestro, que normalmente es quien inicia la conexión, el resto de unidades Bluetooth en la piconet se denominan esclavos. Cualquier dispositivo puede realizar las funciones de maestro y esclavo, pero un mismo dispositivo únicamente puede ser maestro de una piconet.

El maestro es el dispositivo de una piconet cuyo reloj y patrón de saltos se utilizan para sincronizar a todos los demás dispositivos esclavos. Todas las unidades que participan en una piconet están sincronizadas desde el punto de vista del tiempo y de la secuencia de saltos entre canales. Cada unidad dispone de un reloj de sistema interno que determina la temporización y la secuencia de saltos que debe seguir el transceptor.

La topología Bluetooth se puede describir como una estructura de piconets múltiples. Dado que la especificación Bluetooth soporta conexiones punto a punto y punto a multipunto, se pueden establecer y enlazar varias piconets en forma de scatternet.

Las piconets pertenecientes a una misma scatternet no están coordinadas y los saltos de frecuencia suceden de forma independiente, es decir, todos los dispositivos que participan en la misma piconet se sincronizan con su correspondiente tiempo de reloj y patrón de saltos determinado. El resto de piconets utilizarán diferentes patrones de saltos y frecuencias de relojes distintas, lo que supone distintas velocidades de salto entre canales.

Aunque no se permite la sincronización de diferentes piconets, los dispositivos pueden participar en diferentes piconets gracias a una multiplexación por división de tiempo (TDM). Esto permite a un dispositivo participar de forma secuencial en diferentes piconets, estando activo en sólo una piconet cada vez [2].

1.6. Dispositivos y modelos de uso

- ✓ **Dispositivos que incorporan tecnología Bluetooth**

La tecnología Bluetooth permite la comunicación inalámbrica y el intercambio de información entre dispositivos de diversa naturaleza que cumplen las especificaciones del estándar.

A continuación, se muestran dispositivos de uso cotidiano que incorporan tecnología Bluetooth organizados por categorías:

- Audio: Auriculares estéreo, manos libres auriculares.

- Automóvil: Sistemas integrados, manos libres, módulos GPS.

- Ordenadores Personales: Ordenadores portátiles con Bluetooth integrado, adaptadores USB Bluetooth, gateways de acceso a otras redes.

- Periféricos: Teclados y ratones inalámbricos, impresoras.

- Telefonía y Ordenadores de bolsillo: Teléfonos móviles, smart phones, PDAs.

- Video e Imagen: Cámaras de fotos, cámaras de video, proyectores. [2]

- ✓ **Escenarios y modelos de uso de Bluetooth**

La posibilidad de conectar diferentes dispositivos entre sí e intercambiar voz y datos ofrece una amplia gama de escenarios y aplicaciones prácticas de Bluetooth en la vida cotidiana. A continuación se presentan una serie de modelos:

- Intercambio de archivos e información sincronizada entre ordenadores personales, ya sean equipos de sobremesa, ordenadores portátiles, PDAs o smart phones: Bluetooth permite la transferencia de archivos entre dispositivos gracias al perfil OBEX FTP. De esta forma, podemos transferir a un PC las fotografías tomadas con la cámara de un teléfono móvil, copiar las notas tomadas a mano sobre una PDA o simplemente transferir archivos de video y audio a otro equipo.

Así mismo, también es posible sincronizar elementos tales como la agenda de contactos o el calendario de tareas con un teléfono móvil o una PDA.

- Conexión con periféricos sin necesidad de cables: Bluetooth permite establecer un enlace de radiofrecuencia de corto alcance ideal para la conexión de dispositivos periféricos en un rango inferior a 10 metros. Existen multitud de periféricos que emplean tecnología Bluetooth, como teclados, ratones, impresoras, lápices digitales, módems, etc.

Así mismo, también existe una amplia gama de impresoras capaces de recibir por Bluetooth la foto a imprimir desde un teléfono móvil o una cámara digital directamente, sin necesidad de utilizar un ordenador como medio de interconexión.

- Función de Manos Libres para conversaciones telefónicas, ya sea a través de auriculares, kits de automóvil o sistemas integrados: Bluetooth hace posible conversar por teléfono móvil sin necesidad de utilizar las manos para sujetar el terminal cerca del oído. Los auriculares Bluetooth actúan como interfaz de entrada y salida de voz y permiten libertad de movimiento con las manos, al tiempo que mantienen la confidencialidad de la llamada. Existen varios formatos disponibles, como los modelos adaptables a la oreja y las gafas de sol.

Los kits de automóvil Bluetooth recogen y proyectan la voz en el interior del vehículo y permiten al conductor mantener conversaciones por teléfono sin necesidad de apartar las manos del volante.

Las marcas más prestigiosas de la industria del automóvil ya incorporan tecnología Bluetooth en sus coches, permitiendo al conductor integrar funciones del teléfono móvil con el resto de controles del vehículo. De esta forma, cuando el terminal recibe una llamada telefónica el sistema detiene la función de radio/CD y pasa a proyectar por los altavoces la conversación, asegurando que el conductor no tenga que apartar las manos del volante.

- Sistemas de navegación GPS (Global Positioning System): Bluetooth ofrece un medio de comunicación inalámbrico de corto alcance ideal para el envío de coordenadas NMEA geoposicionales entre los módulos receptores GPS y los equipos visualizadores de mapas como PDAs o teléfonos móviles.

- Marketing de proximidad por envío de publicidad: Algunas compañías ya han comenzado campañas de publicidad en las calles basadas en el envío masivo de publicidad directa al teléfono móvil a través de Bluetooth. Emplean dispositivos emisores colocados en puntos estratégicos de elevado tránsito de personas capaces de enviar en un rango de 100 metros paquetes de publicidad personalizados que se adecuan al modelo de teléfono móvil que recibe la información. Algunos ayuntamientos han comprobado el éxito de este tipo de estrategias y han instalado sistemas de envío de información en puntos de interés general, como zonas turísticas, aeropuertos e intercambiadores de transporte público, edificios históricos y museos [2].

1.7. Características del Bluetooth

La principal característica que lleva a la radiofrecuencia a ser superior sobre otras comunicaciones inalámbricas, es transmitir información con la ventaja de superar obstáculos entre el emisor y receptor. La tecnología Bluetooth es una especificación que presenta seguridad en el intercambio de datos y su principal objetivo es reemplazar los cables que conectan unos dispositivos con otros por medio de un enlace de radio universal y de corto alcance.

1.7.1. Canales de transmisión

La tecnología Bluetooth está constituida por un transmisor-receptor, que opera en la banda 2,4 GHz, bajo la tecnología de radio conocida como espectro disperso (transmite y recibe en la frecuencia de 2,4 GHz desde 2,402 GHz hasta 2,480 GHz en saltos de 1 MHz); además, utiliza un esquema de modulación por desplazamiento de frecuencia con filtros gausianos (*GFSK, Gaussian Frequency Shift Keying*).

En la modulación GFSK, un 1 binario representa una desviación positiva de la portadora nominal de la frecuencia; mientras que un 0 representa una desviación negativa de la misma. Después de cada paquete enviado, los dispositivos Bluetooth conectados re-sintonizan su radio transmisor a una frecuencia diferente, saltando de un canal de radio a otro, a una alta velocidad (1600 saltos/segundo); ésta técnica se le conoce como espectro disperso con salto en frecuencia (*FHSS, Frequency Hopping Spread Spectrum*); de esta

manera, los dispositivos Bluetooth utilizan toda la banda de 2,4 GHz y si una transmisión se interfiere sobre un canal, una retransmisión ocurrirá sobre un canal diferente, siempre y cuando esté libre.

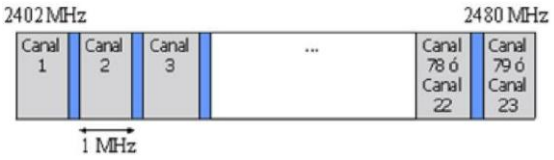


Figura 1.4 Canales de transmisión Bluetooth

En cada canal, se realiza una transmisión de datos durante una ranura de tiempo, cuya duración es de 625 µs. Los datos enviados por los dispositivos, se intercalan durante el tiempo en el que dura la conexión entre ellos, que puede ser cada 1, 3, 5 o un número impar de ranuras.

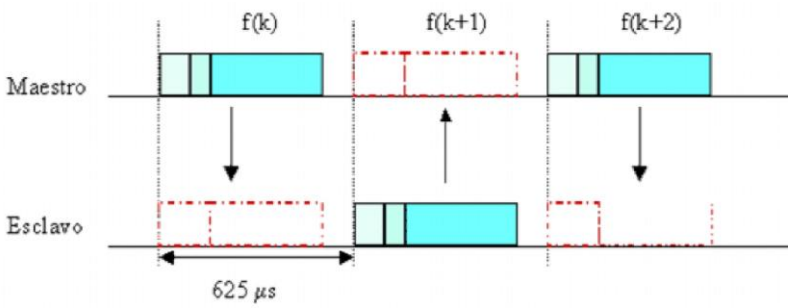


Figura 1.5 Transmisión de paquetes por slot de tiempo

1.7.2. Transmisión de datos

Bluetooth en materia de velocidad de transmisión, soporta nominalmente hasta 1Mbps (con la especificación actual) para el traslado de datos y dependiendo de la clase de enlace se puede tener: una transferencia de 721 kbps en un sentido y 57,6 kbps en la dirección de retorno (para un enlace asimétrico) ó hasta 432,6 kbps en ambos sentidos (para un enlace simétrico). Estas velocidades están limitadas para cierto tipo de aplicaciones como por ejemplo video en tiempo real, en tanto que para la transferencia de archivos e impresión, estas son perfectas.

- ✓ **Datagrama del Bluetooth**

El Datagrama Bluetooth, es la información que se intercambia entre dos unidades y está conformado por un conjunto de datos integrados por: el código de acceso, cabecera y carga útil. Se han definido tres tipos de paquetes para el datagrama Bluetooth, los cuales pueden formarse por: sólo el Código de Acceso, el Código de Acceso y la Cabecera ó el Código de Acceso, la Cabecera y la Carga Útil.

Figura 1.6 Formato de paquete

- ✓ **Código de acceso del Datagrama Bluetooth**

Se deriva de la identidad maestra del dispositivo y se usa para la sincronización, la compensación del offset, la paginación y la búsqueda de equipos Bluetooth. Está formado por 72 bits, cuando el datagrama lo conforman: el Código de Acceso y la Cabecera, pero si el datagrama sólo contiene el Código de Acceso, éste se compone únicamente por 68 bits.

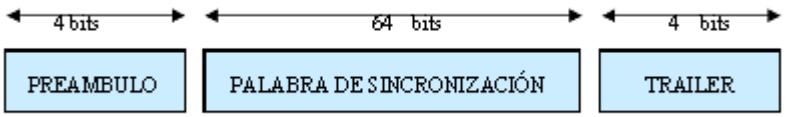


Figura 1.7 Formato del Código de Acceso

El preámbulo es un modelo fijo de 4 bits alternados entre ceros y unos, usados para facilitar la compensación de offset ó DC.

La secuencia del preámbulo depende del bit menos significativo de la palabra de sincronización; si éste es 1, la secuencia del preámbulo será 1010; pero si dicho bit es 0, la cadena estará dispuesta por 0101, tal como se puede apreciar en la figura 1.8

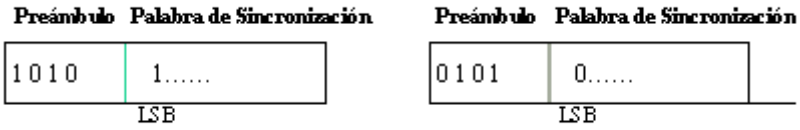


Figura 1.8 Formato del Preámbulo

La palabra de sincronismo, es una palabra código de 64 bits, derivada de la parte baja de dirección maestra del dispositivo Bluetooth (*LAP, Low Address Part*), formada por 24 bits. La cola junto con los tres bits más significativos de la palabra de sincronización, forman un conjunto de ceros y unos alternados, que se usan para prolongar la compensación de offset. La secuencia de la cola puede ser 1010 ó 0101, dependiendo si el bit más significativo de la palabra de sincronización es 0 ó 1 respectivamente, lo cual se puede observar en la figura 1.9

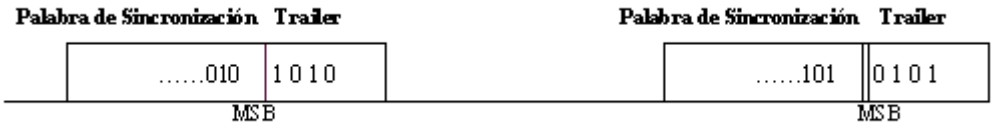


Figura 1.9 Formato del Trailer del Código de Acceso

Existen tres tipos de código de Acceso y estos son:

- Código de Acceso al Canal (CAC): identifica una única Piconet y es incluido en todos los paquetes intercambiados en el canal.
- Código de Acceso de Dispositivo (DAC): es usado para procedimientos especiales de señalización como paginación y respuesta de equipos Bluetooth.
- Código de Acceso de Búsqueda o Indagación (IAC): hay dos variaciones, un código de indagación general (GIAC), que se usa para la búsqueda de otras

unidades Bluetooth dentro del alcance y otro código de acceso de indagación dedicado (DIAC), que es usado para la búsqueda de un grupo de dispositivos que comparten características en común.

- ✓ **Cabecera del Datagrama Bluetooth**

Constituida por 54 bits y contiene información para el reconocimiento de paquete, numeración de paquetes , reordenación de paquetes fuera de orden, el control de flujo, dirección de esclavo y control de errores de la cabecera, repartidos en 6 campos principales, los cuales son:

- AM_ADDR: 3 bits de dirección de miembro activo.
- TIPO: 4 bits de tipo de código de paquete.
- FLUJO: 1 bits de control de flujo.
- ARQN: 1 bits de confirmación de recepción.
- SEQN: 1 bit de número de secuencia.
- HEC: 8 bits de chequeo de error de cabecera.

La cabecera total consiste en 18 bits, tal como se observa en la figura 1.10, y es codificado con corrección de error hacia adelante (FEC) con una tasa de 1/3, resultando una cabecera de 54 bits.

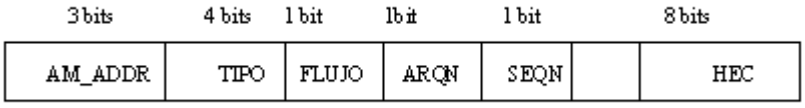


Figura 1.10 Formato de la Cabecera

- ✓ **Carga útil del Datagrama Bluetooth**

Formada por bits desde 0 hasta 2745 y puede contener campos de voz, campos de datos o ambos. Si el payload tiene un campo de datos, la carga útil contendrá también una cabecera de la carga útil.

1.7.3. Tipos de transferencia de datos

Existen dos tipos de transferencia de datos entre dispositivos: Los orientados a conexión de tipo síncrono (*SCO, Synchronous Connection Oriented*) y los no orientados a conexión de tipo asíncrono (*ACL, Asynchronous Connectionless*).

- ✓ **SCO (Síncrono Orientado a la Conexión)**

Es un enlace simétrico punto a punto entre un maestro y un solo esclavo en una Piconet. El maestro mantiene el enlace de SCO usando slots reservados. El enlace respectivo lleva principalmente información de voz y el maestro puede mantener hasta tres enlaces SCO simultáneos; mientras que los esclavos pueden mantener sólo dos enlaces de SCO con diferentes maestros ó hasta tres enlaces SCO con el mismo maestro. Los paquetes de SCO no se retransmiten nunca y se usan para transmisiones de 64 kbps. Es una conexión capaz de soportar voz en tiempo real y tráfico multimedia.

Figura 1.11 Enlace síncrono orientado a la conexión

- ✓ **ACL (Asíncrono Sin Conexión)**

Es un enlace punto a multipunto entre el maestro y todos los esclavos que participan en una Piconet. En los slots no reservados para los enlaces de SCO, el maestro puede establecer un enlace ACL con cualquier esclavo, inclusive con el esclavo ya comprometido en un enlace SCO y sólo puede existir un único enlace ACL. Es una conexión utilizada para tráfico de datos, sin garantía de entrega en donde se retransmiten los paquetes. La máxima velocidad de envío es de 721 Kbps en una dirección y 57,6 kbps en la otra.

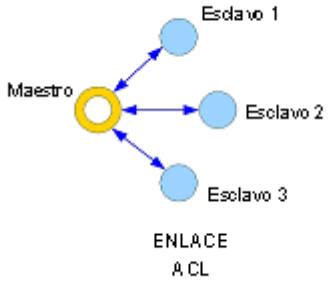


Figura 1.12 Enlace asíncrono sin conexión

PAQUETES			
TIPO	SIMETRICO	ASIMETRICO	
		ENVIO	RETORNO
DM1	108,8	108,8	108,8
DH1	172,8	172,8	172,8
DM3	256	384	54,4
DH3	384	576	86,4
DM5	286,7	477,8	36,3
DH5	432,8	721	57,6

Tabla 1.2 Tipos de velocidades de transmisión de paquetes

1.8. Hardware del Bluetooth

Para alcanzar el objetivo de bajo consumo de potencia y bajo costo, se ideó una solución que se puede implementar en un solo chip, utilizando circuitos CMOS. De esta manera, se logra crear una solución muy compacta y que consume menos energía que un teléfono celular común.

El hardware que compone el dispositivo Bluetooth está formado por dos partes esenciales:

- Un dispositivo de radio, encargado de modular y transmitir la señal.
- Un controlador digital, compuesto por: una unidad central de procesos (CPU), un procesador de señales digitales (*DSP - Digital Signal Processor*), llamado Link Controller *o controlador de Enlace* y de las interfaces con las cuales se conectan los dispositivos anfitriones.

El Controlador de Enlace está encargado de hacer el procesamiento de la banda base y del manejo de los protocolos de solicitud de respuesta inmediata (*ARQ, Automatic Repeat reQuest*) y corrección de errores hacia adelante (*FEC, Forward Error Correction*); además, se encarga de las funciones de transferencia de datos tanto asíncrona como síncrona, codificación de audio y encriptación de datos.

La Unidad Central de Procesos del dispositivo, se encarga de atender las peticiones relacionadas con el dispositivo Bluetooth invitado y así simplificar su operación, para ello, sobre el CPU corre un software denominado Administrador de Enlace ó Link Manager, que tiene la función de comunicarse con otros dispositivos por medio del Protocolo de Administración de Enlace (*LMP, Link Manager Protocol*).

Entre las tareas realizadas por el Controlador de Enlace (LC) y el Administrador de Enlace (LM), destacan las siguientes:

- Envío y Recepción de Datos.
- Emparejamiento y Peticiones.
- Determinación de Conexiones.
- Autenticación.
- Negociación y determinación de tipos de enlace.
- Determinación del tipo de cuerpo de cada paquete.

- ✓ **Direccionamiento de equipos bluetooth**

Se asignan cuatro tipos de direcciones a las diferentes unidades Bluetooth:

- ❖ **BD_ADDR, (Bluetooth Device Address)**

La Dirección de Dispositivo Bluetooth, es única para cada transceptor y está establecida por un conjunto de 48 bits, los cuales son designados por cada fabricante, similar a la dirección MAC de las tarjetas de red (NIC) de los computadores, a fin de mantener una comunicación coherente entre los dispositivos en el momento del enlace Bluetooth.

- **AM_ADDR, (Active Member Address)**

La Dirección de Miembro Activo, es un número de 3 bits y sólo es válido cuando el esclavo está activo en el canal de la Piconet.

- **PM_ADDR, (Parked Member Address)**

La Dirección de Miembro Estacionado, es una dirección de 8 bits que distingue a los esclavos estacionados ó inactivos dentro de la Piconet, lo que significa que no están transmitiendo información por el canal.

- **AR_ADDR, (Access Request Address).**

La Dirección de Petición de Acceso, es usada por el esclavo inactivo, para determinar la ventana o el slot de acceso que le permite enviar una petición de acceso hacia una unidad maestra y sólo es válido cuando el esclavo está inactivo en el canal y no es necesariamente única.

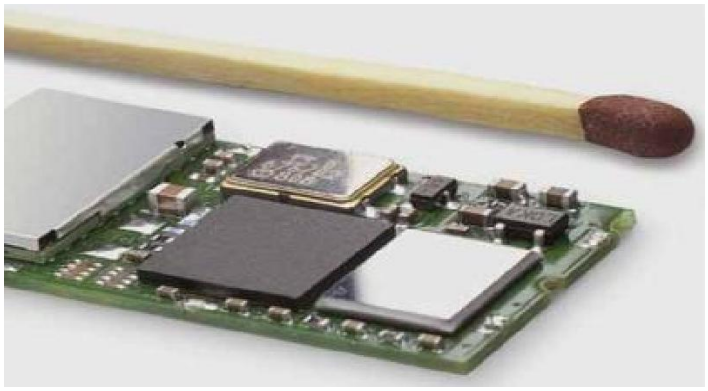


Figura 1.13 Chip del Bluetooth comparado con la longitud de un cerillo de fósforo

1.9. Software del Bluetooth

Para ampliar la compatibilidad entre dispositivos Bluetooth, los equipos que se agregan al estándar, utilizan diferentes protocolos y una interfaz denominada de Control de Host (*HCI, Host Controller Interface*) entre el dispositivo anfitrión (PC, teléfono celular, etc.) y el dispositivo maestro como tal (chip Bluetooth).

Los protocolos son un conjunto de reglas ó normas asociadas a un modelo, que permiten el intercambio de información entre dispositivos de forma segura y ordenada.

- ✓ **Versiones de la especificación bluetooth**

Las versiones existentes de la especificación Bluetooth, han ido evolucionando de conformidad con el avance de la tecnología, entre ellas se encuentran:

- ❖ **Versión 1.1**

La versión 1.1 contiene las especificaciones básicas y conocidas para cada dispositivo Bluetooth, diseñado como un chip transceptor de bajo costo, bajo consumo energético y corto alcance, el cual varía entre 10 y 100 metros. Ideal para redes inalámbricas personales de corto alcance que usan la banda frecuencia libre, que oscila entre los 2,402 GHz y 2,48 GHz. En esta versión, Bluetooth soporta un canal de datos y tres canales para la transmisión de voz. El canal de datos puede intercambiar información a una velocidad aproximada de 721 kbps, usando una conexión punto a punto o una conexión multipunto con encriptación de datos.

- ❖ **Versión 1.2**

Provee una solución inalámbrica complementaria para co-existir Bluetooth y WiFi en el espectro de los 2,4 GHz, sin interferencia entre ellos. La versión 1.2 usa la técnica de salto de frecuencia adaptivo (*AFH, Adaptive Frequency Hopping*), que ejecuta una transmisión más eficiente y un método seguro para el encriptamiento de datos.

La versión 1.2, ofrece una calidad de voz (*Voice Quality - Enhanced Voice Procesing*) con menor ruido ambiental, y provee una rápida configuración de la comunicación con los otros dispositivos Bluetooth dentro del rango del alcance, como por ejemplo: PDAs, HIDs (*Human Interface Devices*), computadores portátiles y de escritorio, headsets, impresoras y celulares.

❖ **Versión 2.0**

La versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica de transmisión de datos reforzada (EDR, *Enhanced Data Rate*), que le permite mejorar las velocidades de transmisión hasta 3 Mbps; además, se ha logrado reducir el número de pasos para conectar dos aparatos Bluetooth en pocos segundos, aumentando su seguridad. La reducción de consumo se ha conseguido gracias a la función de "indagación valorada del canal (Sniff Subrating)", que aumenta la duración de la batería cinco veces más que las especificaciones anteriores.

1.10. Perfiles del Bluetooth

✓ **Perfiles genéricos del Bluetooth**

El SIG Bluetooth ha identificado varios modelos de uso del estándar de comunicaciones Bluetooth, cada uno de los cuales está acompañado por un *perfil*. Los perfiles definen los protocolos y características que soportan un modelo de uso particular. Esto garantiza la interoperabilidad, ya que si dos dispositivos de distintos fabricantes cumplen con la misma especificación del perfil Bluetooth, podemos esperar que interactúen correctamente cuando se utilicen para un uso particular.

Un perfil define los mensajes específicos y procedimientos usados para implementar una característica. Algunas características son obligatorias y algunas pueden ser opcionales.

Se definen cuatro perfiles genéricos que contienen la especificación de los perfiles específicos: el Perfil de Acceso Genérico (GAP, Generis Access Profile), el Perfil de Puerto Serie (SPP, Serial Port Profile), el Perfil de Aplicación de Descubrimiento de Servicios (SDAP, Service Discovery Application Profile) y el Perfil Genérico de Intercambio de Objetos (GOEP, Generic Object Exchange Profile).

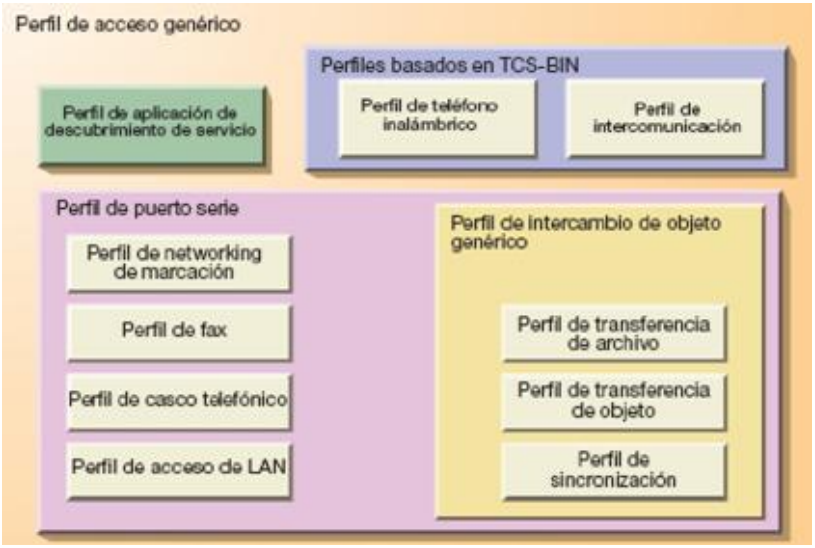


Figura 1.14 Perfiles de Bluetooth

- **Perfil de Acceso Genérico**

El Perfil de Acceso Genérico (GAP, Generis Access Profile) define los procedimientos generales para descubrir dispositivos Bluetooth, así como los procedimientos de gestión de enlace para establecer una conexión entre dos dispositivos Bluetooth.

El Perfil GAP debe implementarse en cualquier dispositivo Bluetooth para asegurar la interoperabilidad básica y la coexistencia con otros dispositivos, independientemente del tipo de aplicación que soporten. Los dispositivos que además cumplan otro perfil Bluetooth pueden emplear adaptaciones de los procedimientos genéricos, tal como se especifiquen en ese perfil. Sin embargo, deben seguir siendo compatibles con el perfil GAP en el nivel de procedimientos genéricos.

- **Perfil de Puerto Serie**

Cuando la tecnología inalámbrica Bluetooth se utiliza para sustituir al cable, se emplea el Perfil de Puerto Serie (SPP, Serial Port Profile) para el canal resultante orientado a la conexión. Este perfil está construido sobre el Perfil de Acceso Genérico y define cómo deben configurarse los dispositivos Bluetooth para emular una conexión a través de un cable serie utilizando RFCOMM, un protocolo de transporte sencillo que emula los puertos serie RS-232 entre dispositivos homólogos.

Las aplicaciones ejecutadas en los dispositivos son normalmente aplicaciones heredadas que esperan que la comunicación tenga lugar a través de un cable serie. Cualquier aplicación heredada puede ser ejecutada sobre cualquiera de los dos dispositivos utilizando el puerto serie virtual como si los conectara un cable físico, con señalización de control RS-232; pudiendo necesitar la ayuda, en algunos casos, de una aplicación auxiliar que utilice la especificación Bluetooth a ambos lados del enlace.

- **Perfil de Aplicación de Descubrimiento de Servicios**

El Perfil de Aplicación de Descubrimiento de Servicios (SDAP, Service Discovery Application Profile) describe las características y procedimientos utilizados para descubrir servicios registrados en otros dispositivos Bluetooth y obtener información acerca de esos servicios.

El Perfil SDAP utiliza el Protocolo de Descubrimiento de Servicios SDP, incluido en la pila de protocolos Bluetooth, para localizar los servicios disponibles en dispositivos situados dentro del radio de acción de un dispositivo Bluetooth. El procedimiento de descubrimiento de servicios en dispositivos próximos no es automático, se requiere que el usuario invoque específicamente al protocolo SDP mediante la Aplicación de Descubrimiento de Servicios. Una vez que se crea el enlace con un dispositivo determinado, se pueden localizar los servicios que ofrece y estos pueden ser seleccionados a través del interfaz de usuario según el tipo de aplicación que se desee ejecutar.

El protocolo SDP permite realizar dos tipos de operaciones relacionadas con el descubrimiento de servicios en dispositivos Bluetooth:

- Búsqueda de servicios (*Service Searching*): permite localizar dispositivos cercanos que ofrezcan un servicio específico.
- Enumeración de servicios (*Service Browsing*): permite conocer los servicios ofrecidos por un determinado dispositivo.

❖ **Perfil Genérico de Intercambio de Objetos**

El Perfil Genérico de Intercambio de Objetos (GOEP, Generic Object Exchange Profile) define cómo deben soportar los dispositivos Bluetooth los modelos de uso de intercambio de objetos. Incluye tres perfiles asociados a modelos de uso específicos basados en el protocolo OBEX (OBject EXchange): el Perfil de Transferencia de Archivos (OBEX File Transfer), el Perfil de carga de objetos (OBEX Object Push) y el Perfil de Sincronización.

OBEX permite escenarios de conexión rápida: transferencia-desconexión (OBEX Object Push) y también permite el establecimiento de sesiones en las que las transferencias tienen lugar durante un período de tiempo, manteniendo la conexión incluso cuando esté inactiva (OBEX File Transfer).

El uso principal de OBEX se realiza en aplicaciones de carga y descarga de archivos. Se basa en el modelo cliente/servidor. Bajo el Perfil Genérico de Intercambio de Objetos, un cliente carga o envía objetos de datos en un servidor mediante la operación PUT del protocolo OBEX; o bien descarga o recibe objetos de datos desde un servidor mediante la operación GET del protocolo OBEX. [2]

✓ **Perfiles Bluetooth para modelos de uso**

Se han identificado cuatro perfiles genéricos (GAP, SPP, SDAP y GOEP), sobre los que se definen los diferentes perfiles específicos para modelos de uso. Estos perfiles Bluetooth para modelos de uso son múltiples y variados, y se implementan de manera opcional e independiente por cada fabricante y tipo de dispositivo.

La especificación Bluetooth 1.0 define los siguientes perfiles:

- Perfil de Telefonía Inalámbrica (CTP, Cordless Telephony Profile)
- Perfil de Intercomunicación (IP, Intercom Profile)
- Perfil de Puerto Serie (SP, Serial Port Profile)
- Perfil de Acceso Telefónico a Redes (DUN, Dial-Up Networking)
- Perfil de Auriculares (HS, HeadSet Profile)

- Perfil de Fax (FP, Fax Profile)
- Perfil de Acceso a Red (LAP, LAN Access Profile)
- Perfil de Transferencia de Archivos (FTP, File Transfer Profile)
- Perfil de Carga de Objetos (OPUSH u OPP, Object Push Profile)
- Perfil de Sincronización (Sync, Synchronization Profile)

Adicionalmente, los siguientes perfiles han sido recientemente aprobados por el SIG o están en fase de desarrollo:

- ESDP, Extended Service Discovery Profile
- A2DP, Advanced Audio Distribution Profile
- AVRCP, Audio Video Remote Control Profile
- BIP, Basic Imaging Profile
- BPP, Basic Printing Profile
- CIP, Common ISDN Access Profile
- GAVDP, Generic Audio Video Distribution Profile
- HFR, Hands-Free Profile
- HCRP, Hardcopy Cable Replacement Profile
- HID, Human Interface Device Profile
- PAN, Personal Area Networking Profile
- SAP, SIM Access Profile

❖ **Perfil de Acceso Telefónico a Redes**

El Perfil de Acceso Telefónico a Redes (DUN, Dial-Up Networking) define los protocolos y procedimientos utilizados por dispositivos tales como módems y teléfonos móviles para implementar el modelo de uso denominado *puente hacia Internet*. El escenario posible más habitual para este modelo es el uso del teléfono móvil como módem inalámbrico para conectar un PC a un servicio de acceso telefónico a Internet.

❖ **Perfil de Auriculares**

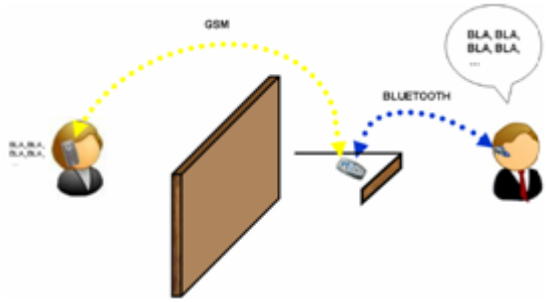
El Perfil de Auriculares (HS, HeadSet Profile) define los protocolos y procedimientos para el modelo de uso que permite utilizar un dispositivo auricular de última generación como

interfaz de entrada y salida de audio de otro dispositivo, generalmente un teléfono móvil o un PC, con el propósito de incrementar la libertad de movimiento del usuario al mismo tiempo que se mantiene la confidencialidad de la conversación.

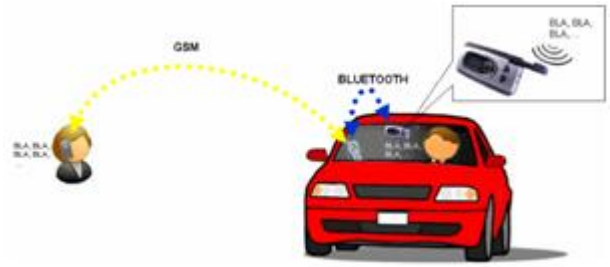
Se definen dos roles para los dispositivos que implementan el Perfil de Auriculares: pasarela de audio y auricular. El dispositivo *pasarela de audio* es aquel que inicia el procedimiento de conexión, mientras que el dispositivo *auricular* se define como el que actúa como mecanismo de entrada y salida de audio remotas para la pasarela de audio.

El modelo de uso del Perfil de Auriculares permite multitud de configuraciones y define tres escenarios de uso habituales:

- Manos Libres Auriculares (Hands-Free HeadSet) conectado a un teléfono móvil: Permite al usuario mantener conversaciones telefónicas sin necesidad de acercar el terminal al oído. Su empleo puede extenderse a comunicaciones con PCs, para aplicaciones de VoIP (Voz sobre IP) como *Skype*.



- Manos Libres de automóvil (Hands-Free Car Kit) conectado a un teléfono móvil: Permite al usuario mantener conversaciones telefónicas en el interior de un vehículo sin necesidad de apartar las manos del volante para sostener el teléfono móvil.



- Pasarela de audio entre dos dispositivos Bluetooth cualesquiera: Permite a un usuario configurar dos equipos Bluetooth, que no tienen porqué tratarse de auriculares, sino simples PCs o PDAs, y establecer una pasarela de audio entre los dos, de forma que el audio que reproduce el software de un dispositivo, se transmite al otro dispositivo a través del enlace SCO (Synchronous Connection Oriented) y puede ser proyectado por los altavoces del segundo. Así mismo, el audio recogido por el micrófono de un dispositivo se transmite al otro dispositivo, donde puede ser grabado en un archivo de sonido.

❖ **Perfil de Fax**

El Perfil de Fax (FP, Fax Profile) define los protocolos y procedimientos utilizados por aquellos dispositivos que implementen la parte de fax del modelo de uso llamado *punto de acceso a datos en redes WAN*. Un teléfono móvil o un módem que utilice tecnología Bluetooth pueden ser utilizados por un PC como dispositivo *fax* inalámbrico para enviar y recibir mensajes de fax.

❖ **Perfil de Acceso a Red**

El Perfil de Acceso a Red (LAP, LAN Access Profile) define cómo los dispositivos Bluetooth pueden acceder a los servicios de una LAN (Local Area Network) utilizando

el protocolo PPP sobre RFCOMM, y cómo puede utilizarse el mismo protocolo PPP para conectar en red dos dispositivos utilizando Bluetooth. En este modelo de uso, varios terminales de datos utilizan un punto de acceso a la red (LAP, LAN Access Point) como conexión inalámbrica a una red de área local, de forma que operan como si estuviesen conectados a la red directamente.

PPP (Point to Point Protocol) es un estándar de la IETF utilizado ampliamente como medio de acceso a redes. Aunque PPP es capaz de soportar varios protocolos de red (IP, IPX, etc.), el Perfil de Acceso a Red no obliga al uso de ningún protocolo en particular.

El Perfil de Acceso a Red simplemente define cómo se soporta PPP para proporcionar acceso a la LAN a uno o múltiples dispositivos Bluetooth y para establecer una comunicación PC a PC utilizando conexiones PPP sobre una emulación de cable serie a través de RFCOMM.

- **Perfil de Transferencia de Archivos**

El Perfil de Transferencia de Archivos (FTP, File Transfer Profile) soporta el modelo de uso de *transferencia de archivo*s a través del protocolo OBEX File Transfer, el cual ofrece la capacidad de transferir objetos de datos (archivos y carpetas) de un dispositivo Bluetooth a otro, así como navegar por los contenidos de las carpetas del dispositivo remoto.

Los dispositivos que implementan el Perfil de Transferencia de Archivos pueden actuar como cliente o como servidor. El dispositivo *cliente* es aquel que inicia la operación de envío o extracción de objetos al y desde el dispositivo *servidor*.

El *servidor* es el dispositivo Bluetooth remoto que proporciona un servidor de intercambio de objetos a través de los comandos OBEX.

Los servidores pueden imponer políticas de restricción de permisos de lectura y escritura, para evitar la creación y borrado de carpetas y archivos.

Se definen las siguientes operaciones en el Perfil de Transferencia de Archivos:

- Navegar por la jerarquía de carpetas.
- Listar el contenido de una carpeta.
- Extraer objetos, mediante el comando GET.
- Enviar objetos, mediante el comando PUT.
- Borrar objetos.

❖ **Perfil de Carga de Objetos**

El Perfil de Carga de Objetos (OPUSH u OPP, Object Push Profile) define los requisitos de aplicación para implementar el modelo de uso de *carga de objetos* a través del protocolo OBEX Object Push, el cual ofrece la capacidad de cargar y descargar objetos de datos de un dispositivo Bluetooth a otro.

Inicialmente, el Perfil de Carga de Objetos se utilizaba para cargar y descargar objetos tales como citas en formato *vCalendar* o tarjetas de visita en formato *vCard* de otro dispositivo, lo que permitía el intercambio de tarjetas de visita entre dos dispositivos Bluetooth. Actualmente, el perfil conserva esta funcionalidad, aunque también se utiliza para transferencia rápida de archivos.

❖ **Perfil de Sincronización**

El Perfil de Sincronización define los requisitos para los protocolos y procedimientos utilizados por las aplicaciones que proporcionan el modelo de uso de *sincronización*. El modelo proporciona sincronización dispositivo a dispositivo de programas de gestión de la información personal (PIM, Personal Information Management).

La información que manejan estos programas consiste normalmente en una agenda de teléfonos de contactos, calendario, mensajes y notas.

Los dispositivos que implementan el Perfil de Sincronización pueden actuar como cliente y servidor. Las unidades activas en el modelo de uso de *sincronización* deben soportar tres funciones: sincronización, comando de sincronización y sincronización automática.
La sincronización en Bluetooth debe soportar al menos una de las siguientes clases de aplicación:

- Sincronización de agendas telefónicas
- Sincronización de calendarios
- Sincronización de mensajes
- Sincronización de notas

Para conseguir la interoperabilidad a nivel de aplicación, se definen formatos de contenido específicos para cada unidad activa. Estos formatos de contenido son los siguientes: *vCard, vCalendar*, *vMessage* y *vNote*.

La función de comando de sincronización permite a un dispositivo cliente trabajar como un servidor y recibir un comando de sincronización desde otro dispositivo cliente.

La función conocida como sincronización automática permite a un dispositivo cliente iniciar la sincronización cuando el dispositivo servidor entra dentro de su rango de cobertura. En el nivel de banda base, esto significa que el cliente realiza una búsqueda del servidor a intervalos regulares, y cuando detecta que éste ha entrado en su rango de cobertura comienza la sincronización [2].

CAPÍTULO II

PROTOCOLOS DE SEGURIDAD

2.1. La pila de protocolo Bluetooth

Uno de los principales objetivos de la tecnología bluetooth es conseguir que aplicaciones de diferentes fabricantes mantengan una comunicación fluida. Para conseguirlo, receptor y transmisor deben ejecutarse sobre la misma pila de protocolos [8].

.

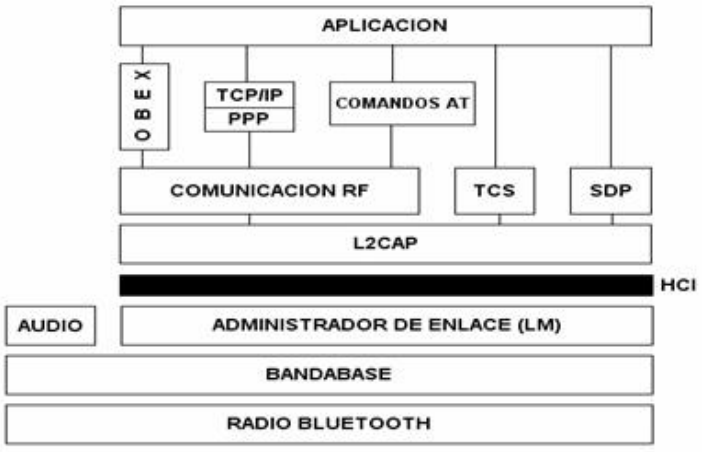


Figura 2.1 Pila de Protocolos

La pila está constituida por dos clases de protocolos. Una primera clase llamada de protocolos específicos que implementa los protocolos propios de Bluetooth. Y una segunda clase formada por el conjunto de protocolos adoptados de otras especificaciones. Esta división en clases en el diseño de la pila de protocolos de Bluetooth permite aprovechar un

conjunto muy amplio de ventajas de ambas. Por un lado, al implementar protocolos específicos de Bluetooth permite utilizar los beneficios que aporta la adopción de la tecnología Bluetooth. Por otro lado, la utilización de protocolos no específicos ofrece la ventaja de la interacción de esta tecnología con protocolos comerciales ya existentes. Así como la posibilidad de que Bluetooth este abierto a implementaciones libres o nuevos protocolos de aplicación de uso común.

La pila de protocolos se puede dividir en cuatro capas lógicas:

- Núcleo de Bluetooth: Radio, Banda Base, LMP, L2CAP, SDP
- Sustitución de cable: RFCOMM
- Protocolos adoptados: PPP, UDP, TCP, IP, OBEX, WAP, IRMC, WAE
- Control de telefonía: TCS-binary, AT-Commands

Pese a que el núcleo de bluetooth fue desarrollado en su totalidad por la SIG, algunos protocolos como RFCOMM y TCS-binary han sido desarrollados siguiendo las recomendaciones de otras instituciones de telecomunicaciones [9].

2.1.1. Capa Banda Base

La capa Banda Base, maneja los canales y los enlaces físicos; además de otros servicios como: la corrección de errores, blanqueo de datos, selección del salto de frecuencia y seguridad de Bluetooth. La capa Banda Base se encuentra sobre de la capa de radio en la pila de protocolos y funciona como un Controlador de Enlace, que trabaja con el Administrador del Enlace, para llevar a cabo la conexión con otros dispositivos y el control de potencia del transmisor.

La capa Banda Base controla enlaces asíncronos y enlaces síncronos, maneja paquetes, realiza paginación y búsqueda para el acceso de dispositivos Bluetooth, averiguando las unidades que se encuentran dentro del área de cobertura.

El transceptor de Banda Base aplica un esquema de división de tiempo dúplex (TDD), de forma que, transmite y recibe información simultáneamente.

- ✓ **Paquetes de la capa banda base**

Todos los datos en la Piconet se transmiten en paquetes y existen varios tipos definidos para la capa Banda Base.

Todas las capas superiores usan estos paquetes para constituir la PDU (*Protocol Data Unit*) de nivel superior y son:

- ID, NULL, POLL, FHS, DM1, que se definen tanto para enlaces SCO como para enlaces ACL.
- DH1, AUX1, DM3, DH3, DM5, DH5 se definen solo para enlaces ACL.
- HV1, HV2, HV3, DV se definen solo para enlaces SCO.

Los paquetes tienen un formato específico, representado en la Figura 1.6, así pues, cada paquete se compone de 3 entidades, el código del acceso (72 bits), la cabecera (54 bits), y la carga útil (de 0 a 2745 bits), explicados anteriormente.

- ❖ **Paquete ID.-** La identidad o paquete ID, consiste en el código de acceso del dispositivo (DAC) ó código de acceso de indagación (IAC) y tiene una longitud fija de 68 bits. Este paquete se usa, por ejemplo, en procesos de búsqueda, indagación y rutinas de respuesta de dispositivos Bluetooth.

- ❖ **Paquete NULL.-** El paquete NULO, no tiene ningún payload y por consiguiente sólo se compone por el código de acceso al canal y la cabecera del paquete. Su longitud total es de 126 bits y es usado primordialmente para devolver información acerca del éxito de una transmisión anterior hacia el dispositivo maestro.

- **Paquete POLL.-** El paquete POLL es muy similar al paquete NULO, ya que no posee payload, pero en contraste, éste requiere una confirmación del destinatario y es usado en una Piconet por el maestro para registrar a los esclavos, los cuales deben responder aún cuando ellos no tengan información para enviar al canal.

- **Paquete de Sincronización de Salto de Frecuencia (FHS, Frequency Hop Synchronization).-** Es un paquete especial de control, que revela principalmente: la dirección y el reloj nativo del dispositivo Bluetooth remitente. El payload contiene 144 bits de información más un código de 16 bits de Corrección de Errores por Redundancia Cíclica (CRC).

- **Paquete DM1.-** Sirve para soportar mensajes de control en cualquier tipo de enlace y también lleva datos de usuario regulares, puesto que el paquete DM1 es reconocido en el enlace SCO.

- **Paquete HV1.-** El paquete HV1, lleva 10 bits de información y la longitud del payload es de 24 bits fijos. Los paquetes HV, se usan principalmente para transmisión de voz y nunca son retransmitidos. El paquete HV1 puede llevarse a una velocidad de 64 kbps en 1.25 mseg., con lo que es enviado en 2 slots de tiempo alternados.

- **Paquete HV2.-** Lleva 20 bits de información y la longitud del payload se fija en 240 bits. Se usa para la transmisión de voz a una velocidad de 64 kbps en un tiempo de 2.5 mseg., con lo que es enviado cada 4 ranuras de tiempo.

- **Paquete HV3.-** Lleva 30 bits de información y la longitud del payload es fijada en 240 bits. Se usa para transmisión de voz a una velocidad de 64 kbps en 3.75 mseg., con lo que es enviado cada 6 ranuras de tiempo.

- **Paquete DV.-** Es una combinación de paquetes de voz y datos. El payload es dividido internamente en un campo para la voz que corresponde a 80 bits y un campo de datos que contiene 150 bits.

- **Paquete DH1.-** Es similar al paquete DM1, excepto que la información es codificada en el payload y puede llevar 28 bytes de información más un código de 16 bits de corrección de errores por redundancia cíclica (CRC). Se usa para una alta tasa de transmisión de datos y puede cubrirse en una sola ranura de tiempo.

- **Paquete DM3.-** Es un paquete DM1 con un payload extendido. Puede cubrirse en 3 ranuras de tiempo y contiene 123 bytes de información (incluido 2 bytes de cabecera del payload), más un código de 16 bits de CRC.

- **Paquete DH3.-** Este paquete es similar al DM3, sólo que la información en el payload no es codificada. Como resultado el paquete DH3 puede llevar 185 bytes de información (incluyendo 2 bytes de cabecera de payload), más un código de 16 bits de CRC. El paquete DH3 puede cubrir 3 slot de tiempo.

- **Paquete DM5.-** El paquete DM5 es un paquete DM1 con payload extendido y puede cubrir hasta 5 ranuras de tiempo. El payload contiene 226 bytes de información (incluyendo 2 bytes de cabecera de payload), más un código de 16 bits de CRC.

- **Paquete DH5.-** Este paquete es similar al DM5, sólo que la información del payload no es codificada. Este paquete puede llevar hasta 341 bytes de información (incluyendo 2 bytes de cabecera de payload), más un código de 16 bits de CRC. Puede cubrir 5 ranuras de tiempo.

- **Paquete AUX1.-** Se parece al paquete DH1 y puede llevar hasta 30 bytes de información (incluyendo 1 byte de la cabecera de payload), con lo que puede cubrir una sola ranura de tiempo.

✓ **Canales lógicos de la capa banda base**

En el sistema Bluetooth, se definen cinco canales lógicos:

- **Canal de Control LC (Control de Enlace).-** El Canal de Control de Enlace, lleva información de control de enlace, control de flujo y caracterización del payload. El canal LC se lleva en cada paquete, excepto en el paquete ID, que no contiene ninguna cabecera.

- **Canal de Control LM (Administrador de Enlace).-** El Canal de Administración del Enlace, lleva información de control intercambiada entre los administradores del enlace de los dispositivos maestro y esclavo, típicamente el canal LM usa paquetes DM.

- **Canal de Usuario UA/UI (Usuario de Datos Asincrónico/Sincrónico).-** El Canal UA lleva datos de usuarios asincrónicos, transparentes al nivel del Protocolo de Adaptación y Control de Enlace Lógico (L2CAP). Estos datos pueden transmitirse en uno o más paquetes de la capa Banda Base

- **Canal de Usuario US(Usuario de Datos Sincrónicos).-** El Canal US lleva datos de usuarios sincrónicos que se llevan sobre un enlace SCO. El canal US sólo puede dirigirse hacia los paquetes SCO, ya que típicamente los otros canales están dirigidos hacia los paquetes ACL.

✓ **Controlador de enlace de la capa banda base**

El controlador de Bluetooth opera en dos estados principales:

❖ **Standby ó Reserva**

Es un estado donde las unidades Bluetooth consumen un bajo porcentaje de potencia y en el cual su reloj de sincronismo está inactivo; además, no hay interacción con otros dispositivos.

❖ **Conexión**

En este proceso, el maestro y el esclavo pueden intercambiar paquetes, usando el código de acceso al canal y el reloj nativo del maestro, para sincronizar el envío de datos.

Dentro de estos 2 estados principales, se encuentran siete subestados, que son procesos en los que puede encontrarse el controlador de enlace antes de pasar a un estado principal.

Estos subestados se usan principalmente para añadir esclavos o hacer conexiones en la Piconet, y son los siguientes:

- page (paginación)
- page scan (análisis de la paginación)
- inquiry (búsqueda)
- inquiry scan (análisis de la búsqueda)
- master response (respuesta del maestro)
- slave response (respuesta del esclavo)
- inquiry response (respuesta de búsqueda)

✓ **Establecimiento de la conexión**

Normalmente, una conexión entre dos dispositivos Bluetooth ocurre de la siguiente manera:

Cuando la unidad maestra no sabe nada acerca de un equipo remoto, debe seguirse un procedimiento de búsqueda de dicho dispositivo y a continuación, uno de paginación.

Si se conocen detalles de la unidad remota, sólo se necesita realizar el procedimiento de paginación.

- ✓ **Búsqueda**

Permite a un dispositivo maestro: descubrir cuántos equipos están dentro de su cobertura, determinar sus direcciones y sincronizar su reloj nativo con el de las demás unidades.

En este proceso, la unidad fuente envía los paquetes respectivos hacia una unidad invitada y a continuación recibe la respuesta desde este equipo. La unidad destino que recibe los paquetes, estará en un estado de análisis de búsqueda y atenta a recibir peticiones de acceso.

Después de que este procedimiento de búsqueda se ha completado, se puede establecer una conexión, usando el proceso de paginación.

En la figura 2.2 se puede apreciar el intercambio de paquetes de búsqueda entre un dispositivo maestro y un esclavo.

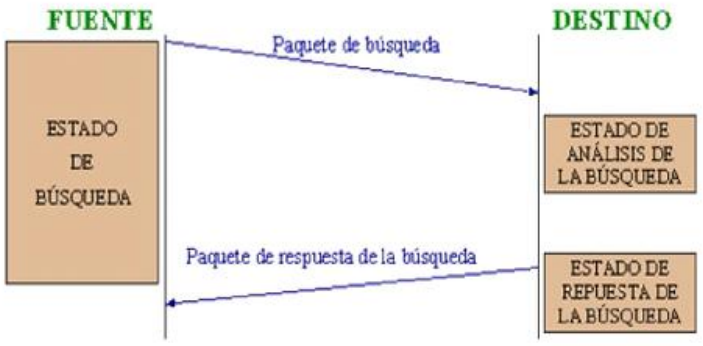


Figura 2.2 Cronograma del procedimiento de búsqueda

- ✓ **Paginación**

En este proceso se puede lograr una conexión verdadera, siguiendo un proceso de búsqueda y sólo se requiere la dirección del dispositivo Bluetooth para establecer dicha conexión. La unidad que establece la conexión, lleva a cabo el procedimiento de paginación y desempeña el papel de maestro dentro del enlace.

El procedimiento de paginación se desarrolla de la siguiente manera:

1. El aparato fuente, pagina el aparato destino. (Estado de paginación).
2. El destino recibe la paginación. (Estado de análisis de la paginación).
3. El destino manda una contestación a la fuente. (Estado de Respuesta del Esclavo).
4. La fuente manda un paquete Sincronización de Salto de Frecuencia (FHS) al destino. (Estado de Respuesta del Maestro).
5. El destino manda una segunda contestación a la fuente. (Estado de Respuesta del Esclavo).
6. El destino y la fuente proceden a intercambiar los parámetros del canal. (Estado de Respuesta del Maestro y Estado de la Respuesta del Esclavo).

En la figura 2.3 se indica el proceso de paginación entre un equipo maestro y el destino, antes de poder establecer una conexión.

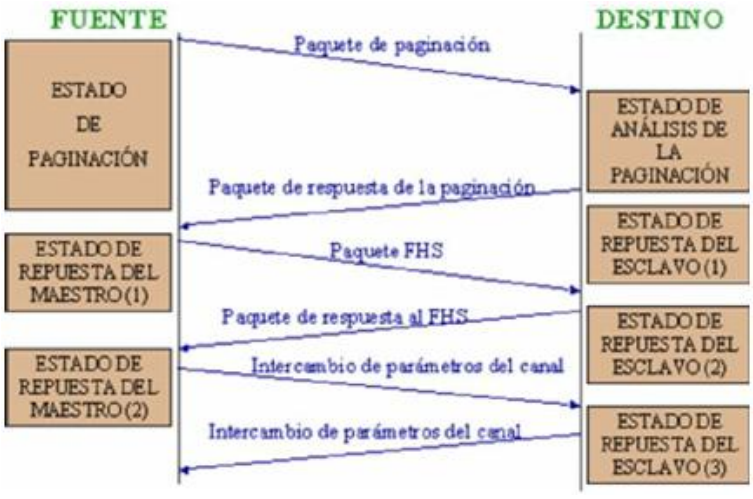


Figura 2.3 Cronograma del procedimiento de paginación

Si el proceso de paginación y búsqueda son exitosos, se entra en un estado de conexión, el mismo que empieza con un paquete POLL (Sondeo), mandado por el maestro, para verificar que ese esclavo se ha sincronizado con el reloj y con el canal de frecuencia del maestro. El esclavo puede responder con cualquier tipo de paquete de confirmación.

- ✓ **Estados de respuesta del controlador de enlace**
  - ❖ **Respuesta de búsqueda**

Cuando un mensaje de búsqueda es recibido con éxito por un esclavo, hay una sincronización del salto de frecuencia entre el maestro y el invitado. Ambos dispositivos entran en una rutina de respuesta para intercambiar información referente al establecimiento del enlace. Es importante que para la conexión de las unidades en la Piconet se use el mismo código de acceso al canal, la misma secuencia de salto al canal y que se sincronicen los relojes internos de los dispositivos.

- ❖ **Respuesta del esclavo**

Después de haber recibido su propio código de acceso, la unidad esclava transmite un mensaje de respuesta, que consiste en enviar al canal el mismo código de acceso en un solo slot de tiempo.

- ❖ **Respuesta del maestro**

Cuando el maestro ha recibido la respuesta del esclavo, éste entrará en la rutina de respuesta del maestro, que se basa en transmitir un paquete de sincronización de salto de frecuencia (FHS), el cual contiene el tiempo del reloj maestro, los 48 bits de la dirección del maestro (BD_ADDR), bits de paridad y la clase del dispositivo.

Después de este envío, el maestro estará presto por una segunda contestación del esclavo, donde reconocerá la recepción del paquete FHS.

❖ **Respuesta de Indagación**

Para el funcionamiento de indagación, hay sólo una respuesta del esclavo y ninguna del maestro. El maestro escucha entre los mensajes de indagación para poder responder cualquiera de ellos, en cambio el esclavo es el que indaga y solicita las respuestas del maestro.

✓ **Examinación del controlador de enlace**

❖ **Examinación de búsqueda**

En este estado, la unidad escucha su propio código de acceso al dispositivo (DAC) para la duración de la ventana de examinación. Durante esta ventana, la unidad escucha un solo salto de frecuencia a la vez.

La secuencia de saltos de búsqueda es determinada por la dirección del dispositivo Bluetooth (BD_ADDR), lo que significa que cada 1,28 seg., se selecciona una frecuencia diferente.

❖ **Examinación de indagación**

Es muy similar al estado de examinación de búsqueda, sin embargo, en lugar de examinar el código de acceso del dispositivo Bluetooth, el receptor examina la longitud suficiente del código de acceso de indagación para inspeccionar cualquiera de las frecuencias de indagación.

✓ **Indagación del controlador de enlace**

En el sistema Bluetooth, se define un procedimiento de indagación para aplicaciones donde la dirección del dispositivo destino es desconocida para la fuente. Alternativamente, el proceso de indagación puede usarse para descubrir otras unidades Bluetooth dentro del área de cobertura.

2.1.2. Interfaz de radio

La capa radio de Bluetooth, es el nivel inferior definido en la especificación, y exige los requisitos necesarios de operación del dispositivo transceptor, para poder enviar la información y funcionar en la banda ISM de acceso público.

2.1.3. Capa de protocolo de Gestión de Enlace (LMP)

LMP (Link Manager Protocol) es el responsable de la configuración y control de enlace entre dispositivos Bluetooth. Cuando dos dispositivos Bluetooth se encuentran dentro del radio de acción del otro, el gestor de enlace (Link Manager) de cada dispositivo se comunica con su homólogo por medio de mensajes a través del protocolo LMP.

Estos mensajes realizan el establecimiento del enlace entre ambos dispositivos. LMP también se encarga de las tareas relacionadas con la seguridad: autenticación y cifrado; generación, intercambio y comprobación de las claves de enlace y cifrado.

2.1.4. Capa de Interfaz de Controlador de Host (HCI)

La capa HCI (Host Controller Interface) actúa como frontera entre las capas de protocolo relativas al hardware (módulo Bluetooth) y las relativas al software (host Bluetooth). Proporciona una interfaz de comandos para la comunicación entre el dispositivo y el firmware del módulo Bluetooth y permite disponer de una capa de acceso homogénea para todos los módulos Bluetooth de banda base, aunque sean de distintos fabricantes.

Una de las tareas más importantes del interfaz HCI es el descubrimiento de dispositivos Bluetooth que se encuentren dentro del radio de cobertura. Esta operación se denomina consulta o *inquiry* y funciona del siguiente modo:

- Inicialmente, el dispositivo origen envía paquetes *inquiry* y se mantiene en espera de recibir respuestas de otros dispositivos presentes en su zona de cobertura.

- Si los dispositivos destino están configurados en modo visible (*discoverable*) se encontrarán en estado *inquiry_scan* y en predisposición de atender estos paquetes.

En este caso, al recibir un paquete *inquiry* cambiarán a estado *inquiry_response* y enviarán una respuesta al host origen con sus direcciones MAC y otros parámetros.

Los dispositivos que estén configurados en modo no visible (*non discoverable*) se encontrarán en modo *inquiry_response* y, por tanto, no responderán al host origen y permanecerán ocultos.

- ✓ **Direccionamiento de dispositivos Bluetooth**

Al igual que en otros estándares de comunicaciones IEEE 802, Bluetooth utiliza direcciones MAC de 6 bytes para el direccionamiento de equipos a nivel de red. De esta forma, un dispositivo queda identificado unívocamente por su dirección MAC, comúnmente denominada *BD_ADDR*.

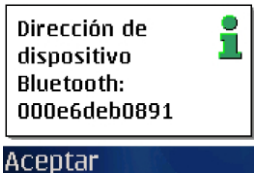


Figura 2.4 Direccionamiento Bluetooth

2.1.5. Capa de protocolo de Adaptación y Control del Enlace Lógico Host (L2CAP)

El Control Lógico del Enlace y el Protocolo de la Capa de Adaptación (L2CAP) están situados sobre la capa Banda Base y reside en capa de enlace de datos. L2CAP proporciona servicios orientados y no orientados a la conexión hacia los protocolos de capas superiores, con capacidades tales como: multiplexación, segmentación y reensamblaje, calidad de servicio y concentración de grupos de datos. L2CAP permite que los protocolos de aplicaciones de niveles superiores, transmitan y reciban paquetes de datos de hasta 64 kb de longitud.

En Banda Base se definen dos tipos de enlace: enlaces Orientados a la Conexión (SCO) y enlaces asíncronos sin conexión (ACL). Los enlaces SCO soportan tráfico en tiempo real de voz, usando un ancho de banda reservado y los enlaces ACL soportan tráfico de datos con retransmisión de paquetes en caso de error o pérdida de los mismos.

La Especificación L2CAP se define sólo para enlaces de ACL y no hay planificada una definición para enlaces de SCO.

- ✓ **Multiplexación de protocolo**

L2CAP debe soportar multiplexación de protocolo y debe ser capaz de distinguir entre protocolos de capa superior tal como el Protocolo de Descubrimiento de Servicio (SDP), RFCOMM, y el Control de Telefonía.

- ✓ **Segmentación y reensamblado**

Los paquetes de datos que exceden la unidad máxima de transferencia (MTU), deben ser segmentados antes de transmitirse. De igual modo, los múltiples paquetes recibidos de Banda Base pueden ser reensamblados en un solo paquete L2CAP más grande. La función de Segmentación y Reensamblado (SAR) es absolutamente necesaria para soportar el uso de protocolos que utilizan paquetes más grandes que los que se usan en Banda Base.

- ✓ **Calidad del servicio**

El proceso de establecimiento de conexión L2CAP permite el intercambio de información dependiendo de la calidad del servicio (QoS) esperada entre dos unidades de Bluetooth.

2.1.6. Capa de protocolo de Descubrimiento de Servicio (SDP)

El descubrimiento de servicios hace referencia a la capacidad de buscar y encontrar servicios disponibles en dispositivos Bluetooth. A través de los servicios, dos dispositivos pueden ejecutar aplicaciones comunes e intercambiar datos.

El protocolo SDP (Service Discovery Protocol) permite a una aplicación cliente obtener información sobre servidores SDP disponibles en otros dispositivos Bluetooth cercanos, enumerar los servicios que ofrecen y las características de dichos servicios. Después de haber localizado los servicios disponibles en un dispositivo, el usuario puede elegir aquel de ellos que resulte más apropiado para el tipo de comunicación que desea establecer.

Un servicio es cualquier entidad que puede ofrecer información, ejecutar una acción o controlar un recurso. Un servicio puede estar implementado como hardware, software o una combinación de hardware y software.

- ✓ **Services Classes**

Un servicio concreto soportado por cierto dispositivo es una instancia de un Services Class o clase de servicio. El Services Class describe los servicios genéricos soportados por un dispositivo:

- Positioning (Location identification)
- Networking (LAN, Ad hoc, ...)
- Rendering (Printing, Speaker, ...)
- Capturing (Scanner, Microphone, ...)
- Object Transfer (v-Inbox, v-Folder, ...)
- Audio (Speaker, Microphone, Headset service, ...)
- Telephony (Cordless telephony, Modem, Headset service, ...)
- Information (WEB-server, WAP-server, ...)

- ✓ **Service Record**

Toda la información relacionada con un servicio que mantiene un servidor SDP está contenida en un *Service Record* o registro individual de servicio.

El protocolo SDP permite realizar dos tipos de operaciones relacionadas con el descubrimiento de servicios en dispositivos Bluetooth: búsqueda y enumeración de servicios.

- La operación búsqueda de servicios (*Service Searching*) permite a un cliente SDP encontrar dispositivos que ofrecen un servicio específico.

- La operación enumeración de servicios (*Service Browsin*) permite a un cliente SDP conocer los servicios ofrecidos por un determinado dispositivo.

En ambos casos, el resultado de la petición SDP devolverá al cliente que la originó una lista de servicios descubiertos acompañada por la definición de los mismos a través de sus *Service Records*.

2.1.7. Capa RFCOMM

El protocolo RFCOMM (Radio Frequency Communication) es un protocolo de emulación de línea serie basado en el estándar ETSI TS 07.10. Proporciona una emulación de los puertos serie RS-232 sobre el protocolo L2CAP.

Este protocolo de "sustitución de cable serie" emula las señales de control y datos RS-232 sobre la banda base, proporcionando capacidades de transporte a los servicios de niveles superiores que utilizan el cable serie como mecanismo de transporte.

Para los propósitos de RFCOMM, un camino de comunicación directa involucra siempre a dos aplicaciones que se ejecutan en dos dispositivos distintos extremos de la comunicación. Entre ellos existe un segmento que los comunica, en este caso, un enlace Bluetooth desde un dispositivo al otro. RFCOMM pretende soportar aquellas aplicaciones que utilizan los puertos serie de los dispositivos donde se ejecutan.

RFCOMM es un protocolo de transporte sencillo que soporta hasta 9 puertos serie RS-232 y permite hasta 60 conexiones simultáneas (canales RFCOMM) entre dos dispositivos Bluetooth.

2.1.8. Protocolo OBEX

OBEX (OBject EXchange) es un protocolo de nivel de sesión desarrollado originalmente por la asociación IrDA (Infrared Data Association) con el nombre de IrOBEX. Su objetivo es soportar el intercambio de objetos de forma simple y espontánea. OBEX se basa en el modelo cliente/servidor y es independiente del mecanismo de transporte, aunque en la implementación de OBEX en la especificación Bluetooth sólo se utiliza RFCOMM como nivel de transporte.

2.1.9. Protocolo adoptados PPP

La especificación Bluetooth emplea varios protocolos existentes que se reutilizan para diferentes propósitos en los niveles superiores. El objetivo de la implementación de estos protocolos es permitir que aplicaciones antiguas funcionen con la tecnología inalámbrica Bluetooth y ayudar a asegurar un correcto funcionamiento e interoperabilidad de esas aplicaciones con aplicaciones modernas diseñadas específicamente para dispositivos Bluetooth.

Bluetooth utiliza el protocolo PPP desarrollado por el IETF (Internet Engineering Task Force), que define cómo se transmiten los datagramas IP sobre enlaces punto a punto, para garantizar la interoperabilidad de dispositivos Bluetooth con aplicaciones basadas en protocolos TCP y UDP en última instancia.

2.1.10. Protocolo adoptados TCP/UDP/IP

Las normas de TCP/UDP/IP se definen para operar en dispositivos Bluetooth que deseen conectarse a través de otras unidades a diferentes servicios o perfiles de Bluetooth, como por ejemplo al Internet a través de una Red de Área Personal (PAN).

2.1.11. Protocolo adoptados WAP

El protocolo de Aplicación Inalámbrica (WAP) es una especificación protocolar inalámbrica, que permite que el usuario se conecte a dispositivos próximos e interactúe con los mismos.

Con un teléfono que posea este protocolo, es posible establecer contacto con un "punto de acceso a informaciones" que suministre datos y noticias relevantes para el ambiente en que se encuentra el usuario. Por ejemplo, un aeropuerto, un centro comercial o un museo. Este punto de acceso también puede servir para acceder a servicios (WAP) generales de Internet.

Otra aplicación podría ser el uso de un teléfono con servicio WAP vía Bluetooth, el cual es usado como control remoto interactivo; donde el usuario puede controlar una unidad Bluetooth navegando por las páginas WAP del dispositivo, las cuales contienen enlaces especiales que activan las funciones o procesos de otros circuitos controlados por el dispositivo. Eso ofrece posibilidades ilimitadas, como por ejemplo la utilización del teléfono como interruptor de luz o llave de una puerta, o incluso para controlar el sistema de alarma doméstico.

2.2. Transferencia de ficheros

Para la transferencia de ficheros se requiere la utilización del protocolo OBEX, que permite el intercambio de objetos de una forma sencilla y que funciona sobre el Protocolo de Comunicaciones por Radio frecuencia (RFCOMM). El Servicio de Descubrimiento de Dispositivos (SDP), es necesario para descubrir el tipo de servicios disponibles para la transferencia de datos, tal como se muestra en la figura 2.5.

Figura 2.5 Pila de protocolos para transferencia de ficheros

2.3. Bridge de Internet

En este modelo se necesita principalmente una pila de protocolos de dos ramas (además de la de SDP), los cuales se usan para acceder a Internet mediante Bluetooth. En una de las pilas tenemos Órdenes AT sobre RFCOMM que son necesarias para controlar el teléfono móvil o módem. En la otra pila encontramos PPP sobre RFCOMM que se precisan para transferir los datos útiles, tal como se muestra en la figura 2.6.

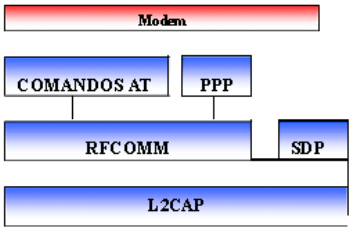


Figura 2.6 Pila de protocolos para el modelo de puente de internet

2.4. Acceso LAN

Esta pila de protocolos se usa para formar parte de una red de área local inalámbrica y es casi idéntica a la del modelo anterior, excepto que no se usan las órdenes AT. La pila de protocolos necesaria para este modelo, se muestra en la figura 2.7.

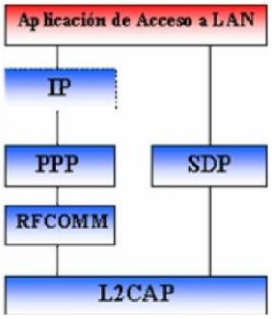


Figura 2.7 Pila de protocolos para el modelo de uso de acceso a LAN

2.5. Protocolos referentes a la seguridad

Existen 4 tipos de redes inalámbricas, la basada en tecnología BlueTooth, la IrDa (Infrared Data Association), la HomeRF y la WECA (Wi-Fi). La primera de ellas no permite la

transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnología HomeRF y Wi-Fi están basados en las especificaciones 802.11 (Ethernet Inalámbrica) y son las que utilizan actualmente las tarjetas de red inalámbricas.

- ✓ **WEP (Wired Equivalent Protocol)**

WEP es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional**.**

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos [10].

- ✓ **OSA (Open System Authentication)**

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable [4].

- ✓ **ACL (Access Control List)**

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso [4].

- ✓ **CNAC (Closed Network Access Control)**

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña [11].

CAPÍTULO III

SIMULACIÓN DE UNA RED BLUETOOTH

3.1. Network Simulator

El ns2 es un simulador de eventos discretos creado para la investigación de redes telemáticas y está disponible en múltiples plataformas. Probablemente ns2 es el simulador de redes gratuito más extendido tanto en investigación como para propósitos docentes.

Este simulador se empezó a desarrollar en 1989 como una variante del simulador Real Network Simulator y ha ido evolucionando substancialmente en los últimos años. En 1995, el desarrollo estaba bajo la supervisión del proyecto VINT (Virtual InterNetwork Testbed), finalmente su investigación acabó en manos de un grupo de investigadores y desarrolladores de la Universidad de California en Berkeley, el LBL (Lawrence Berkeley Laboratory), XEROX Parc y USC/ISI (University of Southern California/ Information Sciences Institute).

Entre los usos más habituales que posee ns2 se puede destacar los siguientes:

- Simular estructuras y protocolos de redes de todo tipo (satélite, wireless, cableadas, etc.)
- Desarrollar nuevos protocolos, algoritmos y comprobar su funcionamiento.
- Comparar distintos protocolos en cuanto a prestaciones.

Ns se está utilizando tanto en entornos de investigación como en entornos educativos. Ns nos va a ser útil para la investigación ya que nos permite acceder a simulaciones con elementos a las que no podríamos acceder normalmente en caso de no disponer de un simulador. También nos permite modificar casi todos los parámetros que influyen en el estado o configuración de una red en tan solo unos segundos mientras que recrear en la realidad este entorno podría costarnos días o incluso meses.

Ns se utiliza en entornos educativos ya que nos permite simular sencillas redes que nos van a ayudar a comprender los distintos protocolos y observar cómo se produce el envió de paquetes entre nodos, etc.

Para definir una simulación en Ns utilizamos un lenguaje de script llamado TCL que nos va a permitir definir los distintos elementos de la red y como debe comportarse. Una vez terminado el script se lo pasamos al Ns y este irá realizando la simulación.

Ns dispone de una interfaz gráfica para visualizar las simulaciones llamada nam (network animator). Nam también dispone de un editor gráfico, que nos va a permitir no tener que usar código TCL para crear las animaciones. Puedes crear la topología de red y simular varios protocolos y fuentes de tráfico mediante el uso del ratón [12].

Es necesario obtener la herramienta UCBT la cual tiene todas las librerías que son necesarias para la simulación de la red Bluetooth, la cual nos permitirá desarrollar de un mejor modo el ambiente grafico de nuestra red.

3.1.1. Instalación de Linux

El software ns2 utilizado en la simulación se puede ejecutar en cualquier versión del sistema operativo Linux.

Es importante mencionar que para una correcta instalación del ns2 se requiere que Linux sea instalado con la opción EVERYTHING (total), de esta manera se copian las librerías necesarias para el correcto desempeño de ns2, caso contrario, se necesitará un conocimiento avanzado acerca de la programación en Linux, para obtener dichas librerías y adjuntarlas en el entorno de trabajo.

3.1.2. Instalación de Network Simulator

Para instalar el simulador ns2 conjuntamente con la librería UCBT, es necesario obtener el paquete "todo en uno del ns2". La versión del ns2 utilizada en el proyecto es ns 2.29.3, para obtener este paquete hay que dirigirse a la siguiente página de Internet http://www.isi.edu/nsnam/. La versión del UCBT utilizada es UCBT 0.9.9.2 para obtener esta librería hay que dirigirse a la siguiente página de Internet http://www.cs.uc.edu/~cdmc/ucbt/src/.

Una vez obtenidos los paquetes ns2 y UCBT, lo primero que se debe hacer es descomprimir el ns2 en el directorio que se desee instalar, en este caso se escogió el directorio raíz dentro de la carpeta home de la siguiente forma:

cd / home

tar zxvf ns-allinone-2.29.3.tar.gz

Luego de descomprimir el paquete se crea el directorio ns-allinone-2.29, aquí se encuentra el directorio ns-2.29, dentro de éste se debe descomprimir la librería UCBT de la siguiente forma:

cd / home

ls

ns-allinone-2.29

cd / home/ns / ns-allinone-2.29 / ns-2.29

tar zxvf ucbt - 0.9.9.2 .gz

Una vez descomprimido el UCBT se debe ingresar a este directorio y ejecutar el siguiente comando:

cd / home/ns / ns-allinone-2.29 / ns-2.29 /ucbt – 0.9.9.2

./install-bt

Para utilizar las herramientas del simulador ns2 es necesario agregar un PATH permanente en el archivo /etc/profile de la siguiente forma:

export PATH=”$PATH:/ simulador/ns-allinone-2.29/bin:/simulador/ns-allinone-2.29/tcl8.4.11/unix:/simulador/ns-allinone-2.29/tk8.4.11/unix

Además se debe realizar los siguientes enlaces simbólicos, a través de estos enlaces se crean puentes hacia los directorios de origen, permitiendo ejecutar estos programas desde cualquier parte:

cd /usr/bin

ln -s /home/ns/ns-allinone-2.29/ns-2.29/ns ns

ln –s / home/ns /ns-allinone-2.29/nam-1.11/nam nam

ln –s / home/ns /ns-allinone-2.29/xgraph-12.1/xgraph xgraph

3.2. Simulación

La simulación del prototipo se basa en una red Ad-hoc punto a punto de corto alcance con tecnología inalámbrica. Los resultados se enfocan a determinar la velocidad efectiva, la relación señal a ruido y niveles de potencia en función de la distancia.

3.2.1. Escenario Bluetooth

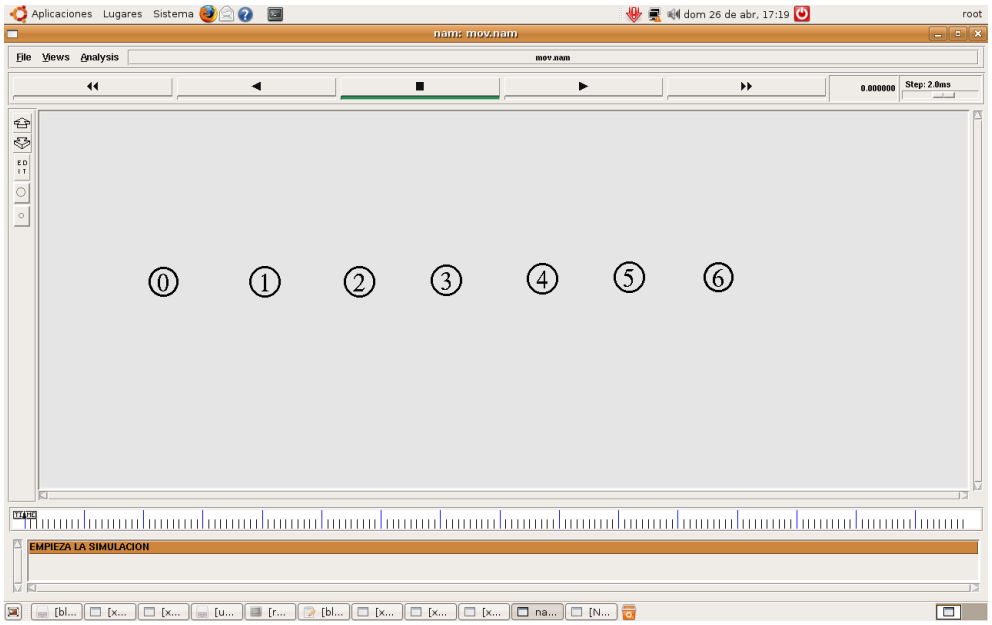


Figura 3.1 Escenario Bluetooth

Simulación Bluetooth

Para tomar las mediciones, se creó siete nodos inalámbricos con tecnología Bluetooth, la comunicación entre estos nodos es unidireccional (enlace simplex).

En la simulación se puede verificar la variación de la velocidad efectiva, la potencia y la relación señal a ruido en función de la distancia. El nodo cero recibirá paquetes TCP con tráfico FTP del nodo uno, luego del nodo dos y así respectivamente hasta el nodo seis.

El script que se utilizó en la simulación es fruto de varios scripts de prueba que se han ido utilizando a lo largo de todo el proyecto. Este código se ha modificado para adecuarlo a las necesidades de este proyecto.

A continuación se muestra el script utilizado para la simulación, en el cual se realiza un comentario de los aspectos más importantes.

SCRIPT BLUETOOTH

Los siguientes comandos permiten almacenar en la variable **v**, la velocidad con la cual se quiere realizar la simulación.

```
#---------------------------------------------------------------------------
#Menu
#---------------------------------------------------------------------------
if {$argc != 1} {
        puts ""
        puts "SELECCIONE LA VELOCIDAD DE TRABAJO:DH1,DH3,DH5,DM1,DM3,DM5"
        puts ""
        exit 1
} else {
        set v [lindex $argv 0]
}
```

Definición de las variables que se utilizan en la simulación como: la capa MAC que en este caso es BNEP para Bluetooth y el número de nodos que intervienen en la simulación.

```
#---------------------------------------------------------------------------
#Declaración de variables a utilizar para la simulación
#---------------------------------------------------------------------------
set val(mac) Mac/BNEP           ;#Variable que identifica el tipo de nodo (BT)
set val(nn)   7                 ;#Variable que especifica el número de nodos BT
```

Se crea una instancia a la clase simulador, para que se pueda realizar la simulación.

```
#---------------------------------------------------------------------------
#Declaraciones típicas de NS2 y NAM
#---------------------------------------------------------------------------
set ns  [new Simulator]                 ;#Definición de ns como nueva instancia de NS2
```

Se configura el nodo con el tipo de MAC definido anteriormente:

```
$ns node-config -macType $val(mac) ;#Definición de nodos a usarse q sean BT
```

Se crean en modo escritura los ficheros que se van a utilizar:

mov.tr: archivo de texto donde se almacenan las trazas generadas en la simulación. Se puede observar la evolución del envío de cada trama. Con este archivo y el

archivo efectiva.pl se logra generar otro archivo que mediante el xgraph permite visualizar como varia la velocidad en función de la distancia.

mov.nam: archivo de texto donde se almacenan las trazas nam, que permiten visualizar el escenario de simulación.

potencia.tr: archivo de texto que se va a generar en la simulación y que mediante el xgraph permiten visualizar como varía la potencia en función de la distancia.

señalruido.tr: archivo de texto que se va a generar en la simulación y que mediante el xgraph permite visualizar como varía la relación señal a ruido en función de la distancia.

```
set tracefile [open mov.tr w]        ;#Definición y creación de un archivo de trazas
set namfile   [open mov.nam w]    ;#Definición y creación de un archivo NAM (ambiente grafico)
set pot       [open ./potencia.tr w]
set SN        [open ./senalruido.tr w]
```

Estos comandos permiten generar las trazas adecuadas tanto en el archivo mov.tr y en el archivo mov.nam y habilitar su uso en el nam.

```
$ns trace-all $tracefile                    ;#Declaración del formato del archivo de trazas
$ns namtrace-all-wireless $namfile 7 7  ;#Declaración del tipo de ambiente y sus dimensiones
Simulator set MacTrace_ ON                  ;#Comando de habilitación para uso del NAM
Simulator set RouterTrace_ ON               ;#Comando de habilitación para el uso wireless en el NAM
$ns color 0 blue
```

Las siguientes líneas permiten crear los siete nodos, asignarles el protocolo de routing AODV, se utilizó este protocolo por ser uno de los más utilizados en este tipo de simulaciones; se activan los nodos a los cero segundos, se establece el tamaño de la cola en 30 paquetes para L2CAP y por último se asignan valores típicos de INQUIRY y PAGE a todos los nodos excepto al nodo 0.

El protocolo de enrutamiento AODV es un protocolo que no requiere que los nodos mantengan las rutas de los destinos que no tienen una conexión activa.

Este protocolo usa números de secuencia de destino para cada ruta de entrada, el número de secuencia del destino es creado por el destino y este es enviado por cualquier ruta de información. Los números de secuencia nos permiten determinar cuál de las diversas rutas es la más accesible.

```
#---------------------------------------------------------------------------
#Creacion de nodos Bluetooth
#---------------------------------------------------------------------------
for {set i 0} {$i < $val(nn) } {incr i} {
   set node($i) [$ns node $i ]
  $node($i) rt AODV                    ;#se asigna el agente de ruteo AODV
  $ns at 0.0 "$node($i) on"            ;#se encienden todos los nodos al mismo tiempo en 0.0seg
  [$node($i) set l2cap_] set ifq_limit_ 30   ;#se establece el tamaño de la cola para la capa L2CAP
  if {$i > 0} {
     $node($i) inqscan 4096 2048       ;#se asignan los valores típicos de inquiry
     $node($i) pagescan 4096 2048      ;#se asignan los valores típicos de page
  }
}
```

Estas líneas asignan al nodo 0 el tipo de modelo inalámbrico adecuado para Bluetooth, la visualización de los paquetes MAC y se configura al Protocolo de Administración de Enlace para que el nodo cero realice una sola vez el INQUIRY

```
$node(0) LossMod BlueHoc        ;#se asigna el tipo de modelo Inalámbrico con o sin pérdidas
$node(0) trace-all-in-air on    ;#se asigna la visualización de tipos de paquetes MAC
[$node(0) set lmp_] set scan_after_inq_ 0  ;#se configura al LMP con comandos para q solo realice
una vez inquiry
```

El procedimiento de configuración del enlace, tráfico y aplicaciones se lo hace para los nodos 1, 2, 3, 4, 5, 6 con el nodo cero.

```
#---------------------------------------------------------------------------
#Configuración de enlace, tráfico y aplicaciones
#---------------------------------------------------------------------------
set tcp0 [new Agent/TCP]          ;#Declaración de un agente de trafico TCP
$ns attach-agent $node(1) $tcp0   ;#Unión del agente con el nodo correspondiente (tx)
set tcp0 [new Agent/TCP]          ;#Declaración de un agente de trafico TCP
$ns attach-agent $node(2) $tcp0   ;#Unión del agente con el nodo correspondiente (tx)
set tcp0 [new Agent/TCP]          ;#Declaración de un agente de trafico TCP
```

```
$ns attach-agent $node(3) $tcp0    ;#Unión del agente con el nodo correspondiente (tx)
set tcp0 [new Agent/TCP]           ;#Declaración de un agente de trafico TCP
$ns attach-agent $node(4) $tcp0    ;#Unión del agente con el nodo correspondiente (tx)
set tcp0 [new Agent/TCP]           ;#Declaración de un agente de trafico TCP
$ns attach-agent $node(5) $tcp0    ;#Unión del agente con el nodo correspondiente (tx)
```

Comandos que permiten generar tráfico FTP sobre la conexión TCP que ya fue creada.

```
set ftp0 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp0 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
set ftp1 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp1 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
set ftp2 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp2 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
set ftp3 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp3 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
set ftp4 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp4 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
set ftp5 [new Application/FTP] ;#Declaración de una aplicación soportada por el agente de trafico TCP
$ftp5 attach-agent $tcp0       ;#Unión de la aplicación al agente de trafico
```

Se define la conducta del nodo destino y se le asigna a la fuente llamada sink.

Este nodo destino es el encargado de generar acks (acuses de recibo) que garantizan el arribo de todos los paquetes al nodo 0.

```
set null0 [new Agent/TCPSink]  ;#Declaración del repositorio del agente de trafico TCP
$ns attach-agent $node(0) $null0  ;#Unión del repositorio con el nodo correspondiente (rx)
```

Se realiza la conexión entre el nodo 0 y el nodo 1.

```
$ns connect $tcp0 $null0    ; #unión del agente de trafico con el repositorio
```

Estos comandos establecen un tamaño de 20 paquetes en el buffer esto indica que si el límite de paquetes es sobrepasado los paquetes serán descartados.

```
set ifq [new Queue/DropTail]  ;#Declaración de la cola o Buffer
$ifq set limit_ 20            ;#Límite de la cola (paquetes)
set ifq1 [new Queue/DropTail] ;#Declaración de la cola o Buffer
$ifq1 set limit_ 20           ;#Límite de la cola (paquetes)
set ifq2 [new Queue/DropTail] ;#Declaración de la cola o Buffer
$ifq2 set limit_ 20           ;#Límite de la cola (paquetes)
set ifq3 [new Queue/DropTail] ;#Declaración de la cola o Buffer
$ifq3 set limit_ 20           ;#Límite de la cola (paquetes)
```

```
set ifq4 [new Queue/DropTail]  ;#Declaración de la cola o Buffer
$ifq4 set limit_ 20            ;#Límite de la cola (paquetes)
```

Variables creadas para iniciar la transferencia de tráfico FTP que son usadas más adelante para generar un efecto de movilidad

```
set nscmd0 "$ftp0 start"
set nscmd1 "$ftp1 start"
set nscmd2 "$ftp2 start"
set nscmd3 "$ftp3 start"
set nscmd4 "$ftp4 start"
set nscmd5 "$ftp5 start"

set nscmd00 "$ftp0 stop"
set nscmd01 "$ftp1 stop"
set nscmd02 "$ftp2 stop"
set nscmd03 "$ftp3 stop"
set nscmd04 "$ftp4 stop"
```

Estas líneas permiten en un tiempo dado iniciar la conexión entre el nodo 0 y los otros nodos indicando el tipo de paquetes que envía y paquetes que recibe, estos paquetes serán ingresados por el usuario que pueden ser: DH5, DH3, DH1, DM5, DM3 y DM1, las velocidades que se alcanzan cuando se transmiten estos paquetes se muestran en la tabla 1.2; también se establece el tamaño de la cola en el buffer que fue definido anteriormente. El tiempo en que se establece la conexión de todos los nodos depende del número de nodos que van a establecer una conexión, para este caso es de 4 segundos.

```
#---------------------------------------------------------------------------
#Organizador de eventos
#---------------------------------------------------------------------------
$ns at 0.1 "$node(0) make-bnep-connection $node(1) $v $v  noqos $ifq"
$ns at 0.2 "$node(0) make-bnep-connection $node(2) $v $v noqos $ifq1"
$ns at 0.3 "$node(0) make-bnep-connection $node(3) $v $v noqos $ifq2"
$ns at 0.4 "$node(0) make-bnep-connection $node(4) $v $v noqos $ifq3"
$ns at 0.5 "$node(0) make-bnep-connection $node(5) $v $v noqos $ifq4"
```

Estas líneas permiten al simulador en un tiempo dado iniciar y terminar la transferencia de datos dando un efecto de movilidad entre el nodo cero y los demás.

```
$ns at 4.0 "$nscmd0"
$ns at 6.0 "$nscmd00"
```

```
$ns at 6.1 "$nscmd1"
$ns at 8.0 "$nscmd01"
$ns at 8.1 "$nscmd2"
$ns at 10.0 "$nscmd02"
$ns at 10.1 "$nscmd3"
$ns at 12.0 "$nscmd03"
$ns at 12.1 "$nscmd4"
$ns at 13.5 "$nscmd04"
```

Al tiempo t=4 segundos se llama a la función record, esta función es la encargada del cálculo del enlace.

```
#--------------------------------------------------------------------------
#Proceso para llamar a la función record para que calcule la potencia y relación señal a ruido
#--------------------------------------------------------------------------
#A los 4.0 segundos llamo a la función record
$ns at 4.0 "record"
```

Se define dos variables locales para la función record la una llamada pot y la otra llamada SN

```
proc record {} {
        global sink pot
        global sink SN
```

Indica la granularidad de 2 segundos y se almacena en la variable time

```
        set ns [Simulator instance]
        set time 2.0
```

Este comando permite determinar en qué tiempo se encuentra la simulación

```
#Cálculo de la distancia
      set now [$ns now]
```

Se calcula la distancia cada 2 segundos debido a que es el tiempo en el cual el nodo va a desplazarse de una posición a otra.

```
      set distancia [expr $now*1.0 - 2.0 ]
```

Se realiza el cálculo de las pérdidas en la trayectoria y el cálculo de la potencia para Bluetooth de acuerdo a las siguientes ecuaciones:

$$L_{patch} = 20\log\left(\frac{4\pi R}{\lambda}\right) \approx 40 + 20\log(R)$$

$$P_{RX}[dB] = P_{TX}[dBm] - L_{patch}[dB] - 8[dB]$$

Ecuación 3.1

Para el cálculo de la potencia de transmisión se toma el valor de 4dBm que es la especificada para la interfaz DBT -122.

```
#Comparo la distancia de acuerdo a una referencia para el cálculo de la potencia.
        if {$distancia <= 8.5} {
#Cálculo de las pérdidas en dB para una distancia menor a 8.5 m
            set perdidas [ expr 40.0 + 20.0*log10($distancia)]
#Cálculo de la potencia
            set potencia [expr 4-pérdidas-8.0]
```

Con la potencia calculada para una distancia menor a 8.5m se calcula la relación señal a ruido. El ruido se cálculo en base a las ecuaciones que se muestran a continuación:

$$PSD = N_0 = KT$$

T = Temperatura absoluta ($^0K = 273^0 + ^0C$)

K = Constante de Boltzman ($1.38 \times 10^{-}23$ J / ºK)

$$N = N_0 AB$$

AB = ancho de banda (hertz)

Ecuación 3.2

Para una temperatura de 27°C y un ancho de banda de 1 MHz correspondiente a Bluetooth y transformando este valor a decibelios se obtuvo un ruido de -154.28 dB.

```
            set sn [expr $potencia+154.28]
```

Se realiza el cálculo de las pérdidas en la trayectoria y el cálculo de la potencia para Bluetooth de acuerdo a las siguientes ecuaciones:

$$L_{patch} = 36\log\left(\frac{4\pi R}{\lambda}\right) - 46.7[dB] \approx 25.3 + 36\log(R)$$

$$P_{RX}[dB] = P_{TX}[dBm] - L_{patch}[dB] - 8[dB]$$

Ecuación 3.3

Para el cálculo de la potencia de transmisión se toma el valor de 4dBm que es la especificada para la interfaz DBT -122.

```
} else {
        set perdidas [ expr 25.3+36*log10($distancia)]
         set potencia [expr 4-$perdidas-8.0]
```

Con la potencia calculada para una distancia mayor a 8.5m se prosigue a calcular la relación señal a ruido como se hizo anteriormente.

```
        set sn [expr $potencia+154.28]
        }
```

Se imprime en el archivo potencia.tr la distancia y la potencia. En el archivo señallruido.tr se imprime la distancia y la relación señal a ruido.

```
puts $pot "$distancia  $potencia    "
puts $SN "$distancia  $sn "
```

Se llama a la función record cada dos segundos, para que realice el cálculo de los parámetros requeridos, esto se debe ya que cada dos segundos se activa el siguiente nodo que se encuentra en una posición diferente.

```
        $ns at [expr $now+$time] "record"
}
```

Se indica el tiempo en el cual la simulación finaliza.

```
$ns at 15.9 "finish"
```

Se llama a la función finish que permite realizar todos los procesos para finalizar la simulación y permite visualizar con el xgraph los resultados obtenidos en la misma.

Para el cálculo de la velocidad efectiva se ejecuta el comando perl que conjuntamente con el archivo efectiva.pl, con el archivo mov.tr, indicando el nodo donde se necesita analizar el resultado y la granularidad generan el archivo velo.tr en el cual se almacena la velocidad efectiva de Bluetooth en función de la distancia. El script efectiva.pl el cual deberá ser guardado en un archivo distinto al programa de la simulación bluetooth con la extensión **.pl**, se muestra a continuación:

SCRIPT efectiva.pl

```
$infile=$ARGV[0];
$tonode=$ARGV[1];
$granularity=$ARGV[2];
#calculamos  cuantos bytes fueron transmitidos durante el intervalo de tiempo especificado
#Por el parámetro granularity en segundos
$sum=0;
$clock=0;
open (DATA,"<$infile")
|| die "Can't open $infile  $!";
while (<DATA>) {
@x= split(' ');
#if ($x[1] >= 4.0)
#{
#columna 1 es el tiempo
if ($x[1]-$clock <= $granularity)
{
#chequeo si los eventos corresponden a recibidos
if ($x[0] eq 'r')
{
#OJO AQUI
#chequeo si el destino corresponde al primer argumento
if ($x[2] eq $tonode)
```

```
{
#chequeo si el paquete es TCP
if ($x[6] eq 'tcp')
{
$sum=$sum+$x[7];
}

}
}
}
else
{       $throughput=8.0*$sum/$granularity;
if ($x[1] >= 4.0)
{
$dis=$x[1] -2. 0;
print STDOUT "$dis $throughput\n" ;
$clock=$clock+$granularity;
$sum=0;
}
}
}
$throughput=8.0*$sum/$granularity;
#       $dis=$x[1] -2. 0;
print STDOUT "$x[1] $throughput\n" ;
$clock=$clock+$granularity;
$sum=0;
close DATA;
#}
exit(0);
```

En esta parte ya se procede a realizar la parte final de la simulación.

```
#---------------------------------------------------------------------------
#Procedimiento final
#---------------------------------------------------------------------------
proc finish {} {
     global node
    $node(0) print-all-stat
    exec nam mov.nam &
    exec perl efectiva.pl mov.tr _0_ 0.1 > velo.tr & \
    exec xgraph velo.tr -t "VELOCIDAD BLUETOOTH vs DISTANCIA" -x "DISTANCIA m" -y "VELOCIDAD bps" &
    exec xgraph potencia.tr -geometry "750x500" -P -t " POTENCIA BLUETOOTH vs DISTANCIA" -x
"DISTANCIA m" -y "POTENCIA dBm" &
    exec xgraph senalruido.tr -geometry "750x500" -P -t "S/N BLUETOOTH vs DISTANCIA" -x
"DISTANCIA m" -y "S/N dBm" &
    exit 0
}
$ns run
```

Ejemplo de Simulación del Prototipo Bluetooth

Para realizar la simulación el usuario debe ingresar al directorio en el cual se encuentran ubicados los scripts bluetooth.tcl y efectiva.pl en este caso los scripts se encuentran en el directorio Bluetooth

Para acceder al directorio se ingreso los siguientes comandos en el terminal de Linux.

cd /Escritorio/Tesis_Tony/Bluetooth/

Para obtener ayuda del uso del script se ingreso el siguiente comando.

ns bluetooth.tcl

Aquí el usuario puede escoger la velocidad para realizar la simulación.

ns bluetooth.tcl DH5

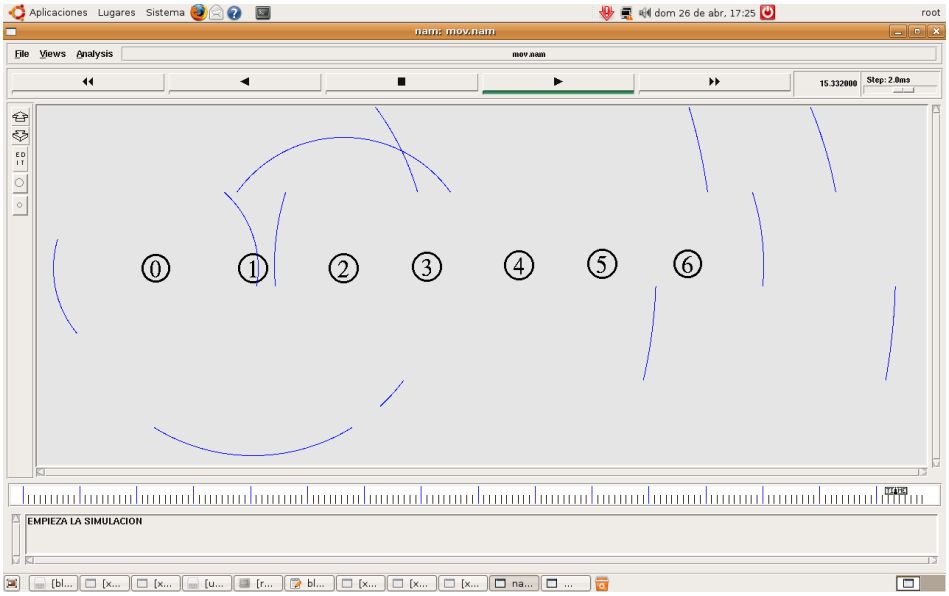


Figura 3.2 Pantalla inicial del nam Bluetooth

Una vez que se ejecute el programa se visualizará el escenario en el nam y los resultados que se obtienen de la simulación en el xgraph como son: potencia, relación señal a ruido y la velocidad efectiva.

Luego de iniciar la simulación en el nam se visualiza como los paquetes son enviados.

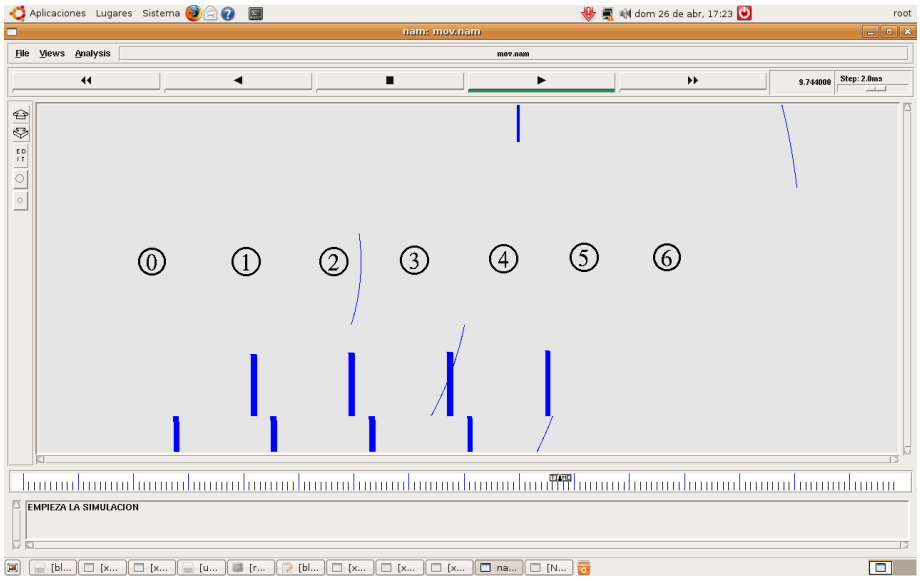


Figura 3.3 Simulación Bluetooth en el nam

Con la ayuda del XGraph y el archivo potencia.tr que se genera en la simulación, visualizamos como la potencia cambia en función de la distancia.

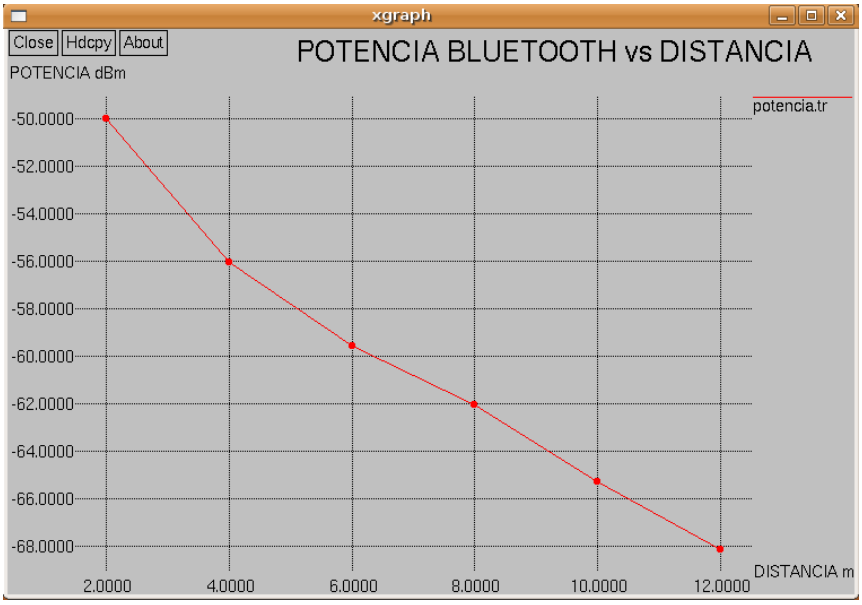


Figura 3.4 Potencia Bluetooth de la Simulación

Con la ayuda del XGraph y el archivo señalruido.tr generado en la simulación, se visualiza la relación señal a ruido en función de la distancia.

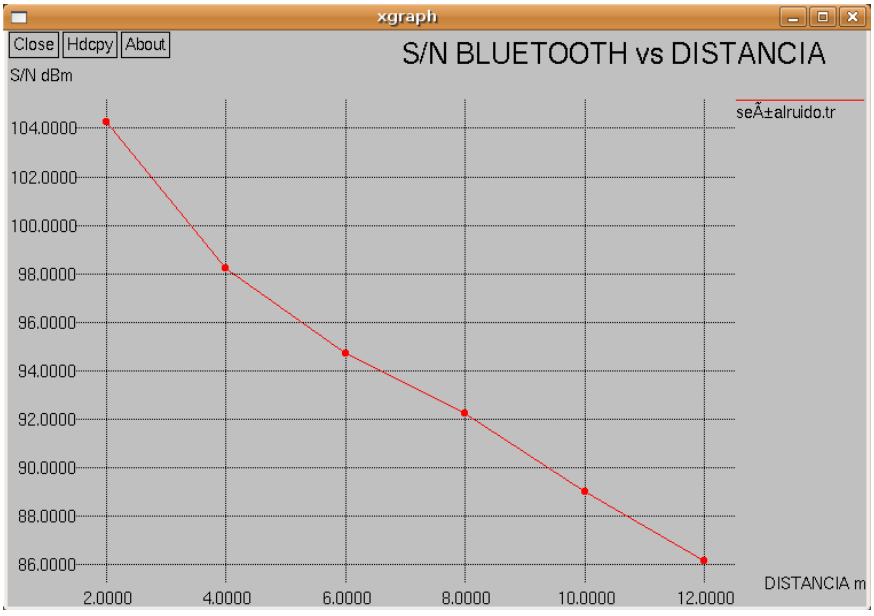


Figura 3.5 Señal a ruido Bluetooth de la Simulación

El archivo efectiva.pl es un programa que permite procesar el archivo blue2.tr generado en la simulación. Este programa permite crear un nuevo archivo con la velocidad efectiva en el nodo que recibe los datos.

Con la ayuda del xgraph y el nuevo archivo creado se genera la siguiente gráfica de la velocidad efectiva para Bluetooth.

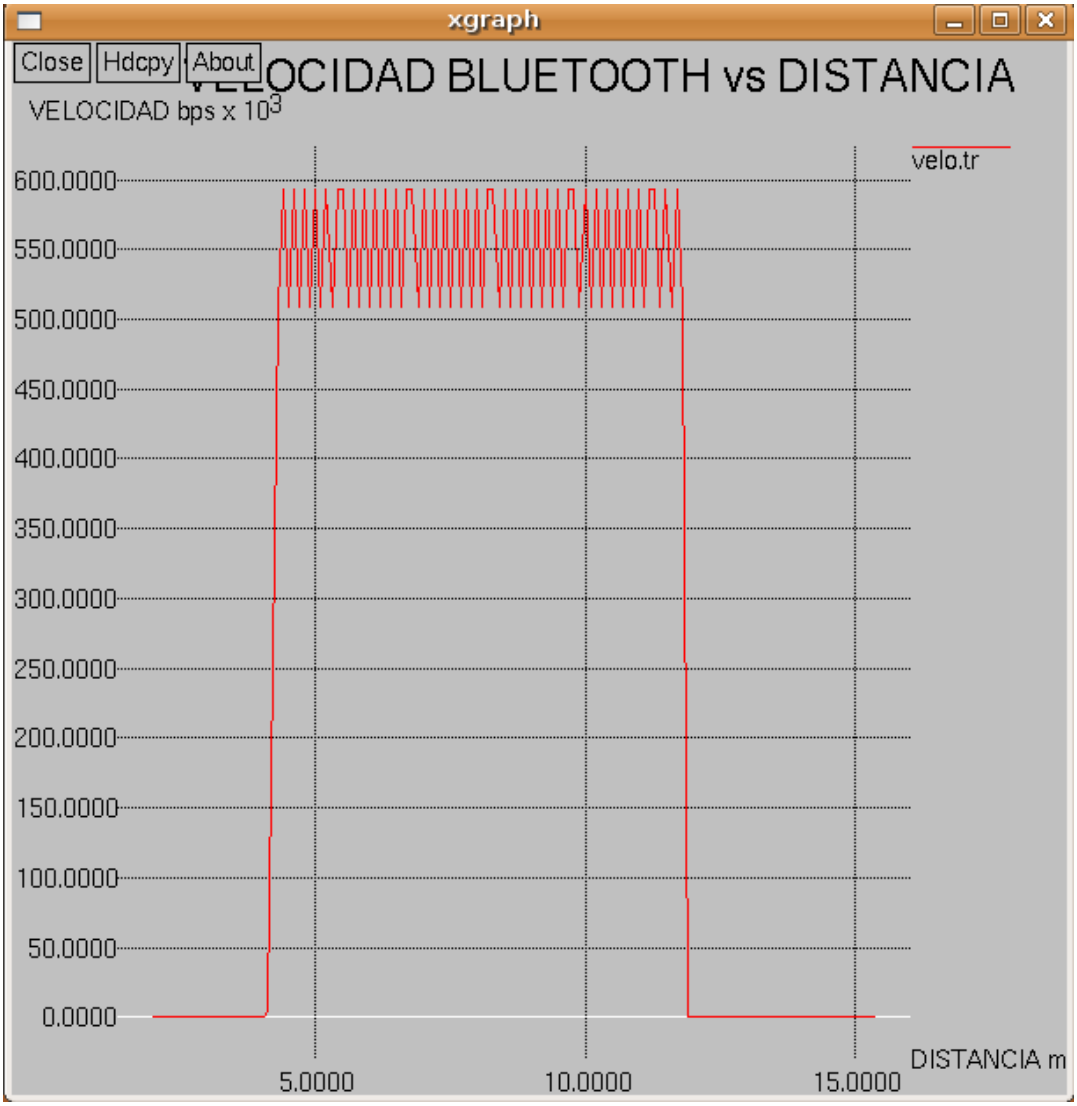


Figura 3.6 Velocidad Bluetooth de la Simulación

3.3. Análisis comparativo de resultados

Mediante la simulación del prototipo se trató de obtener las diferentes respuestas de potencia, señal a ruido, velocidad efectiva. Debido a las limitaciones existentes para la simulación de *Bluetooth* la distancia varía desde los 2 m hasta los 12 m. A continuación se presenta los resultados de la simulación.

La figura 3.4 indica la variación de la potencia en función de la distancia, aquí se observa que a medida que se alejan las estaciones la potencia disminuye tal como ocurre en la realidad.

La figura 3.5 representa la variación de la relación señal a ruido de la simulación en función de la distancia, a medida que se alejan las estaciones la relación señal a ruido decrece.

La figura 3.6 representa la variación de la velocidad efectiva en función de la distancia, en este gráfico se puede observar valores máximos y mínimos de la velocidad esta variación depende de la cola del buffer, es decir si existe congestión en el enlace se emite un mensaje para detener el envió momentáneo de datos.

CAPÍTULO IV

PLANTEAMIENTO DE UN PROTOCOLO DE SEGURIDAD

4.1. Análisis con otras tecnologías

Bluetooth y Wi-Fi cubren necesidades distintas en los entornos domésticos actuales, como la creación de redes y las labores de impresión a la transferencia de ficheros entre PDA's y ordenadores personales, mientras que ZigBee es muy similar al Bluetooth pero con algunas diferencias.

Bluetooth se utiliza principalmente en un gran número de productos tales como teléfonos, impresoras, módems y auriculares. Su uso es adecuado cuando puede haber dos o más dispositivos en un área reducida sin grandes necesidades de ancho de banda. Su uso más común está integrado en teléfonos y PDA's, bien por medio de unos auriculares Bluetooth o en transferencia de ficheros.

Bluetooth tiene la ventaja de simplificar el descubrimiento y configuración de los dispositivos, ya que éstos pueden indicar a otros los servicios que ofrecen, lo que redunda en la accesibilidad de los mismos sin un control explícito de direcciones de red, permisos y otros aspectos típicos de redes tradicionales.

Wi-Fi es similar a la red Ethernet tradicional y como tal el establecimiento de comunicación necesita una configuración previa. Utiliza el mismo espectro de frecuencia

que Bluetooth con una potencia de salida mayor que lleva a conexiones más sólidas. A veces se denomina a Wi-Fi la "Ethernet sin cables". Aunque esta descripción no es muy precisa, da una idea de sus ventajas e inconvenientes en comparación a otras alternativas. Se adecua mejor para redes de propósito general: permite conexiones más rápidas, un rango de distancias mayor y mejores mecanismos de seguridad.

Puede compararse la eficiencia de varios protocolos de transmisión inalámbrica, como Bluetooth y Wi-Fi, por medio de la capacidad espacial (bits por segundo y metro cuadrado) [13].

ZigBee tiene un menor consumo eléctrico, en términos exactos, consume de 30mA transmitiendo y de 3uA en reposo, frente a los 40mA transmitiendo y 0.2mA en reposo que tiene el Bluetooth.

Una red ZigBee puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos, frente a los 8 máximos de una subred (Piconet) Bluetooth.

ZigBee tiene una velocidad de hasta 250 kbps, mientras que en Bluetooth es de hasta 1 Mbps, por tal razón la velocidad de ZigBee se hace insuficiente en aplicaciones para teléfonos móviles, etc., es por eso que se desvía a usos tales como los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor [14].

4.2. Ventajas de los protocolos existentes

WEP (Wired Equivalet privacy)

- Solución estándar incorporada por todos los fabricantes de productos Wi-Fi.
- No necesita de software cliente adicional.
- Encriptación con claves de 40 o 104 bits [15].

Túneles IP

- El protocolo para la encriptación de la información puede ser IPSEC, que es un estándar abierto, lo que permite la compatibilidad con muchos productos.
- Aquí si se puede realizar una autenticación unipersonal y fiable [15].

Filtrado de direcciones MAC

- Creación de una tabla de acceso en cada uno de los puntos de acceso de la red de área local inalámbrica.
- La tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar a una determinada red de área local inalámbrica.
- Sencillo de usar para redes relativamente pequeñas [16].

CNAC (Closed Network Access Control)

- Usa el identificador de la red de área local inalámbrica (SSID, Server Set ID) como contraseña para acceder a la red, tratando de ser un mecanismo de autenticación [16].

4.3. Desventajas de los protocolos existentes

WEP (Wired Equivalet privacy)

- Encriptación poco robusta, sobre todo cuando la clave se utiliza de forma estática.
- Todos los usuarios así como los puntos de acceso de una misma red wireless utilizan la misma clave WEP.
- La clave WEP utilizada puede ser descifrada fácilmente tras varias horas de recopilación de información encriptada con una misma clave WEP.
- La clave WEP se guarda en Windows en un registro que se puede copiar a otra computadora [15].

Túneles IP

- Se requiere de hardware adicional para poder establecer los túneles. Es decir, un equipo o servidor de túneles.
- No es una solución totalmente transparente para el usuario final.
- La encriptación se realiza por software en los clientes, lo que podría ralentizar las comunicaciones.
- Implica encapsular, toda la información transmitida, con un "overhead" adicional.
- No soporta multicast [15].

Filtrado de direcciones MAC

- No es un sistema escalable y flexible, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso.
- El formato de una dirección MAC no es amigable, lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un intruso podría obtener direcciones MAC de tarjetas autorizadas en la red empleando un sniffer y luego asignarle una de estas direcciones a su computadora [16].

CNAC (Closed Network Access Control)

- Fácil de conseguir ya que es enviado por los clientes al asociarse o autenticarse en el punto de acceso, por lo que tampoco garantiza que usuarios no autorizados tengan acceso a la red [16].

4.4. Formulación de un nuevo protocolo

Según como se ha visto en los protocolos de seguridad existentes y estudiado a cada uno podemos formular un nuevo protocolo el cual nos dará un grado más de seguridad que los actuales.

La función de este nuevo protocolo de seguridad será la de realizar una validación de sus direcciones MAC conjuntamente con la autentificación de estas.

La forma en que se realizara este proceso será en que la dirección MAC consta de varios dígitos los cuales uno a uno serán autentificados de una lista de direcciones, la cual llevara un registro de todas las direcciones MAC que tengan acceso a la red.

Una vez realizado este proceso en el cual se garantiza que la dirección es confiable, se deberá ingresar una clave de acceso la cual será única para cada dirección MAC con lo cual evitamos que la red posea una sola clave que pueda ser descifrada para permitir el acceso de direcciones intrusas que puedan ocasionar daños en nuestra red.

Esta clave constara en un registro interno del software o sistema operativo del equipo maestro de la red, el cual variara la clave constantemente para evitar que sea descifrada. Al momento de variar la clave se enviara un código a cada equipo de la red indicando su nueva clave.

Cabe mencionar que este registro interno con las claves de cada dirección MAC tendrá una codificación que solo el equipo maestro sabrá, permitiendo así que solo un usuario tenga acceso a este registro evitando que este sea deliberadamente cambiado provocando problemas de acceso a la red.

Para las direcciones MAC que accedieron a la red después del cambio de clave, el equipo maestro llevara un registro detallado con los tiempos del último acceso del equipo, así este podrá indicar si el equipo estuvo en el cambio de clave o no.

Al asegurarse el sistema que el equipo no recibió su nueva clave, se generara la clave para que el equipo pueda ingresar a la red. Una vez recibido el código el equipo tendrá que reiniciar el proceso de encriptación y autentificación para validar su clave con la cual podrá acceder las veces que desee a la red hasta realizarse nuevamente el proceso de asignación de claves para cada equipo de la red, con lo cual podremos hacer que tenga mayor seguridad logrando así que la red tenga una mayor dificultad para ser descifrada.

A continuación se muestra en la figura 4.1 el diagrama de flujo que indica el proceso de validación y autentificación del nuevo protocolo:

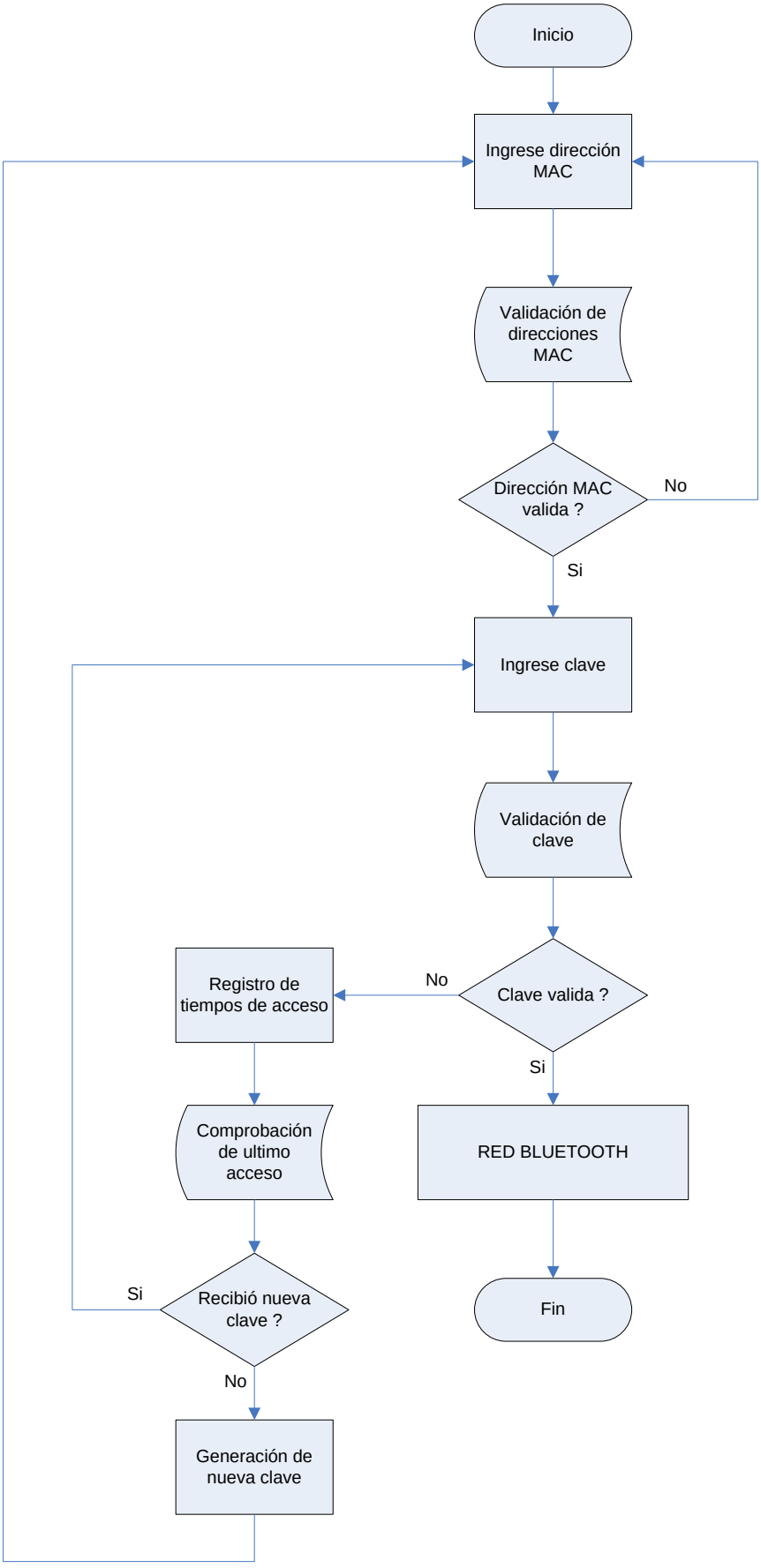


Figura 4.1 Diagrama de flujo del nuevo protocolo

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- En conclusión podemos decir que el protocolo formulado ofrece un mayor grado de seguridad debido a que la generación de claves aleatorias no permite que intrusos puedan descifrar la clave ya que esta permanece en constante variación y si llega a ser descifrada esta ya ha sido variada por el generador de claves.

- Estos análisis nos indican que la potencia, señal a ruido y la velocidad son aspectos que se deberán tomar muy en cuenta para desarrollar nuevas versiones ya que si el bluetooth quiere erigirse como el máximo exponente en comunicaciones inalámbricas tiene que mejorar su capacidad para la transmisión de la información.

- Los protocolos de seguridad son buenos en medida de sus capacidades y la forma en que se los quiera usar pero para aplicaciones que requieren mayor capacidad en la seguridad, estos no son para nada confiables y permiten el acceso de equipos intrusos.

- La tecnología Bluetooth está ganando mayor aceptación con lo cual un mayor número de fabricantes la está aceptando, ya que tiene una disminución significativa

en costos de comercialización lo cual es beneficioso para el usuario que quiere acceder a esta tecnología.

- Bluetooth tiene una mayor robustez frente al ruido que los demás, lo cual hace que sea más estable y seguro y permita que otros sistemas trabajen con esta tecnología.

- Bluetooth permite la conformación de grupos cerrados de usuarios de manera dinámica, este tipo de usuarios operan en redes con infraestructura no fijas, y proporciona una interfaz universal que permite la interoperabilidad entre los diferentes dispositivos, gracias al carácter abierto de la especificación.

- Bluetooth posee la gran ventaja de que está diseñada para entregar servicio inalámbrico a dispositivos de gran movilidad, de reducido tamaño y bajo consumo de potencia que les proporcionen portabilidad e independencia de una fuente de energía fija y que a su vez trabaje en ambiente de corto enlace.

- Para la simulación de la red Bluetooth se utilizó el programa Network Simulator o conocido también como NS2, este es un software que es muy utilizado para simular redes satelitales, redes inalámbricas Ad-Hoc, etc., este simulador es muy confiable para realizar las simulaciones pero es complicado al momento de instalarlo y realizar las distintas simulaciones.

5.2. Recomendaciones

- Se recomienda implementar redes inalámbricas con tecnología Bluetooth en oficinas, lugares cerrados en general que tengan un diámetro no mayor a diez metros y en donde la velocidad de transmisión no sea importante, ya que Bluetooth en distancias menores o iguales a esta, tiene un buen desempeño en lo que corresponde a nivel de potencia, pérdida de datos.

- Se recomienda implementar esta tecnología en lugares que posean dispositivos móviles, celulares, impresoras, PDA`s ya que Bluetooth tiene la capacidad de interactuar con este tipo de dispositivos.

- Se recomienda descargar el paquete completo del programa ***allinone*** del Network Simulator e instalarlo en su totalidad, para evitar problemas en el momento de ejecutar sus librerías.

- Es recomendable tener conocimiento de la herramienta NS2 y de programación, ya que es algo complejo de manejar, en caso de no poseer conocimientos ingresar a algún curso para adquirirlo y poder realizar los diferentes tipos de simulaciones que se pueden realizar en esta herramienta.

- Se recomienda que si el protocolo formulado en la presente tesis va a hacer desarrollado, se debe analizar si es factible su diseño y si su implementación será un aporte para el desarrollo de esta tecnología inalámbrica Bluetooth.

- En cuanto a los protocolos de seguridad es recomendable saber cómo funcionan cada uno de ellos, cuales son sus virtudes y defectos para poder partir de ellos y conjuntamente con el estudio del bluetooth, ir desarrollando futuros protocolos de seguridad que puedan hacer más confiable y seguro a esta tecnología que se está abriendo campo en el mundo de las comunicaciones inalámbricas.

BIBLIOGRAFIA

[1] http://www.alegsa.com.ar/Notas/86.php

[2] http://gospel.endorasoft.es/bluetooth/especificacion-bluetooth/estandar-bluetooth/index.html

[3] http://cvc.cervantes.es/trujaman/anteriores/marzo_01/26032001.htm

[4] http://blog.pucp.edu.pe/category/793/blogid/295

[5] http://es.wikipedia.org/wiki/Bluetooth#El_SIG_de_Bluetooth

[6] http://beta.redes-linux.com/manuales/bluetooth/8-Bluetooth.pdf.gz

[7] http://es.wikipedia.org/wiki/Bluetooth

[8]http://www.unibague.edu.co/portal/programas/ingenieria_electronica/el_oraculo_wlan_wpan/wpan_arquitectura.html

[9] http://www.electronicafacil.net/tutoriales/Protocolos-Bluetooth.html

[10] http://www.monografias.com

[11] www.securitywireless.info

[12] http://linuxalbacete.org/web/content/view/149/31/

[13] http://es.wikipedia.org/wiki/Bluetooth#Bluetooth_vs._Wi-Fi

[14] http://borealtech.wordpress.com/2006/12/20/bluetooth-vs-zigbee/

[15] http://www.virusprot.com/Art43.html

[16] www.cs.cinvestav.mx/Estudiantes/TesisGraduados/2005/tesisLuisDeJesusG.pdf

Fecha de entrega de la Tesis: 3 de Agosto del 2009

_____	_____
Tony Robert Angulo Acunso	Ing. Gonzalo Olmedo
Autor	Director de Carrera