Comunicaciones inalámbricas

TEMA 1 INTRODUCCIÓN A LOS SISTEMAS DE COMUNICACIÓN INALÁMBRICOS

1. REDES DE ORDENADORES

En la definición de una red de ordenadores podemos distinguir cuatro elementos:

- El **protocolo de comunicación**, define el lenguaje y el conjunto de reglas que facilitan la comunicación entre emisor y receptor.
- La **topología** define la manera en que los nodos de comunicación están conectados entre sí.
- La **seguridad** es lo que permite garantizar la confidencialidad, autenticación e integridad de los datos.
- El **medio de transmisión** es el aire, por donde viaja la señal que lleva los datos.

El **espectro electromagnético** es el rango de frecuencia de todas las ondas electromagnéticas que se pueden propagar a través del espacio libre, ordenadas según su longitud de onda y su frecuencia. Los rangos de frecuencia más utilizados son:

- Infrarrojos (IR): Se utilizan en comunicaciones punto a punto de ámbito local, son muy direccionables y no pueden atravesar obstáculos.
- Microondas: Es adecuado para las transmisiones de largo recorrido.
- Radiofrecuencia: Se emplea en las transmisiones de radio y televisión.

2. COMUNICACIONES INALÁMBRICAS

Clasificaremos las distintas comunicaciones inalámbricas atendiendo a su alcance en:

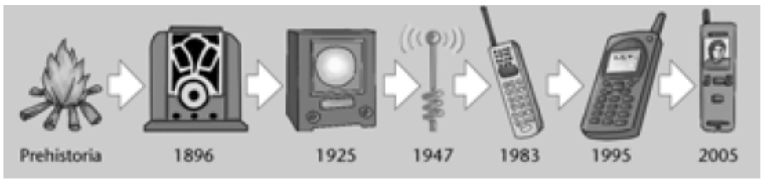
- **Redes de área personal inalámbricas (WPAN)**: Presentan una importante limitación de alcance y por ello los dispositivos tienen que estar poco separados, hay varias tecnologías: DECT, Bluetooth, HomeRF e IrDA.
- **Redes de área local inalámbricas (WLAN)**: Es una red de cobertura geográfica limitada, velocidad de transmisión alta, bajo nivel de errores y administrada de manera privada. Contamos con dos: IEEE802.11 e Hiperlan.
- **Redes de gran alcance inalámbricas (WWAN)**: Permiten la conexión de zonas geográficas distantes.

Las comunicaciones inalámbricas tienen ventajas y desventajas. En el aspecto positivo destacan:

- Accesibilidad y flexibilidad.
- Coste.
- Movilidad.
- Comodidad
- Escalabilidad: Se adaptan fácilmente a los cambios de topología de red.

Como limitaciones tenemos:

- Consumo: Las baterías de los terminales móviles limitan la potencia de transmisión de datos.
- Capacidad de transferencia limitada: el espectro electromagnético es un recurso limitado.
- Calidad: Interferencias y ruidos.
- Seguridad: Cualquiera puede acceder a la información transmitida por el espectro electromagnético sin ningún tipo de limitación.

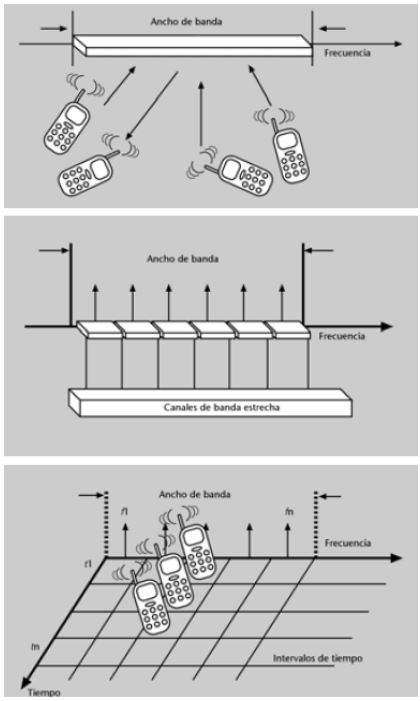


Evolución de las comunicaciones inalámbricas.

TEMA 2 ARQUITECTURAS Y PROTOCOLOS DE LAS COMUNICACIONES INALÁMBRICAS

1. TECNOLOGÍAS DE LA INTERFAZ DE RADIO

En la interfaz de radio tenemos dos clasificaciones generales: las comunicaciones que utilizan banda estrecha y las que emplean difusión de espectro. En la **banda estrecha** a medida que aumenta el número de usuarios que transmiten información, hay que asignar una frecuencia de comunicación para cada uno de ellos, por lo que sus limitaciones son evidentes en sistemas con muchos accesos simultáneos (figura superior de la imagen lateral). Para solucionar este problema se utilizan dos técnicas:



- Acceso múltiple por división de frecuencia: Consiste en dividir el ancho de banda en portadores (canales) de banda estrecha: cuanto más dividimos el ancho de banda en canales, más accesos simultáneos podemos obtener (figura central de la imagen lateral).
- Acceso múltiple por división de tiempo: Se comparte una misma frecuencia que asigna intervalos de tiempo a los usuarios, así se permite combinar una elevada cantidad de señales en una misma portadora, pero hay que ajustar constantemente los intervalos de tiempo para sincronizar las señales en los receptores y los emisores (figura inferior de la imagen lateral).

En las comunicaciones que se utiliza **difusión de espectro**, se utiliza un ancho de banda mayor de lo que se necesita para transmitir la información, y se puede utilizar:

- Salto de frecuencia: Utiliza una portadora de banda estrecha que cambia de frecuencia con un patrón conocido por el transmisor y el receptor, para quién no conozca este patrón la señal aparece como un impulso de ruido de corta duración.
- Secuenciación directa: Se envía un bit de información como una secuencia de bits codificados, el código que se utiliza para codificar la señal es una secuencia de bits denominada chips.

2. REDES PERSONALES INALÁMBRICAS

DECT (Digital enhanced cordless telecommunications) es una transmisión digital inalámbrica que ofrece varias ventajas frente a la tradicional analógica: menos interferencias, más capacidad de dispositivos en una misma zona, más seguridad (cifrado de la información) y más movilidad (se pueden establecer mecanismos para saltar de una red a otra –roaming-). El sistema DECT está formado por dos elementos básicos: la estación fija y el terminal móvil.

Bluetooth es un estándar para conectar sin cables diferentes dispositivos electrónicos, como PDAs, móviles, ordenadores portátiles. Bluetooth define un alcance corto de aproximadamente 10 metros y opcionalmente un alcance medio en torno a los 100 metros. Admite la transferencia de datos y voz y puede soportar diferentes combinaciones de conexiones síncronas (voz) y asíncronas (datos) en función de las necesidades del servicio. En una red Bluetooth cualquier dispositivo puede actuar como máster o como esclavo: el máster se encarga de definir cómo se establece la comunicación físicamente mientras que el esclavo coordina sus transmisiones según las especificaciones del máster. Normalmente el primero que pide el servicio actúa como máster, excepto cuando la red ya ha sido establecida.

HomeRF permite la transferencia inalámbrica de datos y voz y facilita la integración de dispositivos, como el ordenador y la telefonía, la implementación de

sistemas de control del hogar (domótica) activados por voz y la conexión inalámbrica del ordenador con sus periféricos. Para transmitir la voz, se utiliza un sistema de comunicación muy similar al que emplea el DECT y para los datos una tecnología basada en el estándar 802.11.

IrDA ha sido una tecnología que por su bajo coste tanto de implementación como de consumo de potencia se ha ido extendiendo ampliamente. A estas ventajas se añaden que es muy flexible y se adapta fácilmente a una gran cantidad de aplicaciones y dispositivos como PDAs, teléfonos, impresoras… Los dispositivos que utilizan la IrDA se comunican a través del uso del diodo LED que deben estar alineados unos con otros con una desviación máxima permitida de 30º.

3. REDES LOCALES INALÁMBRICAS

Las WLAN son una extensión y/o una alternativa a las LAN con cables. Los usuarios de una WLAN pueden acceder a los recursos que les ofrece la LAN sin tener que depender de infraestructuras de red (cableado, conectores, etc.). Como ventajas tiene la movilidad, instalación simple, flexibilidad, bajo coste y escalabilidad. Pero sus desventajas de centran en la baja velocidad respecto a una red cableada, retrasos, accesos difíciles (hay edificios que atenúan las señales), consumo de los dispositivos, seguridad e interferencias.

Hay dos estándares principales, el IEEE 802.11 y la HiperLAN. El primero de ellos garantiza la funcionalidad de las aplicaciones sin tener que pensar si la comunicación se hace con o sin cables. Hay dos estándares, el IEEE 802.11a que soporta velocidades de hasta 54 Mbps, y el IEEE 802.11b que soporta velocidades de hasta 11 Mbps, también denominado Wi-Fi.

Por otro lado, el hiperLAN es un estándar de redes locales inalámbricas desarrollado por el ETSI. Ofrece una capa PHY capaz de trabajar a velocidad comparables o superiores incluso a las LAN fijas, tiene un esquema de acceso múltiple con calidad de servicio y además ofrece mecanismos para diferenciar redes que se solapen y que utilizan la misma frecuencia sin perder tráfico. La flexibilidad de la arquitectura de la tecnología HiperLAN2 hace que se pueda emplear en muchas de las redes existentes: ATM, UMTS, etc.

4. REDES DE GRAN ALCANCE INALÁMBRICAS

Podemos distinguir dos tipos de WWAN:

- FWWAN (fijas): puede funcionar por radioenlaces o por satélite. La mayor parte de redes de satélites se utilizan para la difusión de la televisión. El uso de estas redes para la transmisión inalámbrica de datos empieza a ser una realidad, pero hay que tener en cuenta los grandes gastos que comportan en equipamiento, los problemas de retraso que se producen la propagarse la señal y el elevado coste por minuto de transmisión.
- MWWAN (móvil): El terminal que envía y recibe la información está en movimiento. Normalmente hay muchos usuarios conectaos simultáneamente que utilizan los servicios en este tipo de redes; por tanto hay que optimizar el uso del espectro radioeléctrico y minimizar la potencia transmitida (para minimizar las interferencias entre canales). En estas redes se tiene un conjunto de estaciones base desplegadas por territorio a las que se quiere dar cobertura conectándolas entre sí o con un centro de conmutación. La estación base de asigna al terminal móvil que recibe con un nivel de potencia mayor, si por la movilidad del terminal otra estación base detecta que recibe una señal de mayor potencia, se produce un cambio de canal y de estación base (handover de potencia). Existe también un handover de calidad.

Encontramos dentro de las redes móviles tres principalmente:

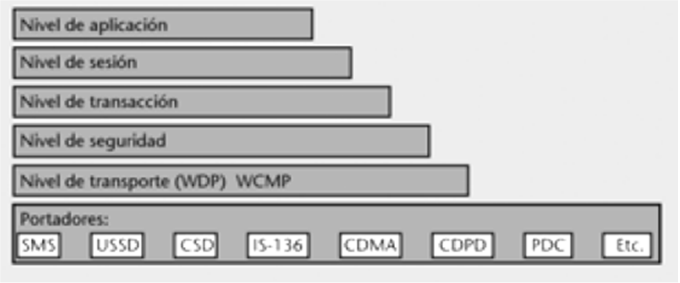
El **GSM** arranca en 1982, cuando se creó un equipo con el nombre groupe special mobile para desarrollar un conjunto de estándares para una red de comunicaciones móviles y se promovió la reserva para este sistema de dos bandas de frecuencias próximas a 900 MHz. GSM ofrece servicios de telefonía, transmisión de datos, fax y envío de SMS. Cuenta con canales de tráfico (voz y datos) a 9,6 Kbps reales, y con canales de control (para sincronización). Normalmente la voz se codifica para reducir los bits que ocupa.

GPRS: Es una tecnología de comunicaciones inalámbrica estandarizada por el ETSI, que corresponde a la generación 2,5G. Es una evolución de la tecnología GSM que utiliza la misma infraestructura que la anterior (bajo coste de implantación) y se basa en la conmutación de paquetes: los usuarios siempre están conectados y los modelos de tarificación se basan en la cantidad de información transmitida y no en el tiempo de conexión.

UMTS: Define una tecnología de comunicaciones inalámbrica optimizada para permitir servicios multimedia de alta velocidad como vídeo, audio y acceso a internet. Cuenta con el apoyo de la mayoría de los operadores de telecomunicaciones y fabricantes, ya que representa una oportunidad única de crear una masa de mercado para servicios multimedia, personalizados y de fácil uso que permitan el acceso móvil a la sociedad de la información. Lo malo es que para hacer la transición de GPRS a UMTS sí es necesario invertir en una nueva infraestructura. Puede operar en modo conmutación de circuitos con conexiones permanentes a la red para servicios de audio y vídeo, y en modo conmutación de paquetes para transferencias de datos y acceso a Internet.

5. WAP

El protocolo WAP fue creado para proporcionar contenidos de Internet y aplicaciones de telefonía avanzadas a los terminales y teléfonos móviles, un mercado que se encuentra en continua expansión. Los terminales WAP presentan una serie de características que condicionan la especificación del protocolo WAP: pantalla reducida, ancho de banda de conexión bajo, conexiones no demasiado estables, dispositivos de entrada reducidos al igual que su memoria, baterías de no muy larga duración… Con todos estos condicionantes se ha tenido que crear un nuevo lenguaje (WML wireless markup language), se ha tenido que implementar un nivel de seguridad y definir un modelo de programación en WAP.



El protocolo WAP tiene una estructura en niveles donde encontramos las siguientes capas:

- Capa de aplicación: Debe establecer las reglas que permitan a los proveedores de servicios la creación de aplicaciones, el funcionamiento de los agentes que hay en los terminales móviles y la interacción con estos servicios o aplicaciones.
- Capa de sesión: Es la interfaz que establece las funciones necesarias para el control de la sesión: establecimiento de la transmisión, control del proceso y finalización de la sesión. Para ello cuenta con capacidad de negociación.
- Capa de transacción: Contiene las especificaciones que aseguran la transmisión de los datagramas del servicio WAP. Funciona de manera similar al tradicional TCP, pero con las modificaciones necesarias para adaptarse a una red inalámbrica: ancho de banda limitado y disponibilidad de recepción no permanente.

- Capa de seguridad: Es opcional y cuando está presente establece las funciones de seguridad en la transmisión, por ejemplo en aplicaciones de comercio electrónico, acceso a datos bancarios, etc.

- Capa de transporte: Conecta la capa de red con las capas superiores y permite que el modelo WAP sea independiente del tipo de operador o tecnología de red empleada para acceder al servicio a aplicación.

TEMA 3 SERVICIOS Y APLICACIONES

1. DISEÑO DE APLICACIONES Y SERVICIOS INALÁMBRICOS

Para conseguir una buena comunicación, el emisor tendría que poder adaptar la información que pretende transmitir a la capacidad de comprensión del receptor. Si pensamos en términos de dispositivos que acceden a una información (móviles accediendo al proveedor de contenidos, por ejemplo), este proveedor ha de diseñar los contenidos teniendo en cuenta el dispositivo mediante el cual el cliente accede a él. Un primer problema a resolver es conseguir que una misma aplicación sea accesible para distintos dispositivos, aprovechando las ventajas y a la vez salvando las limitaciones de cada uno. La solución a este problema es **XML**.

XML permite separar la información de su presentación, de manera que un mismo contenido se puede presentar con distintos formatos. Un documento XML está bien definido o es válido, cuando cumple una DTD determinada, es decir cuando la información se ha etiquetado siguiendo los tipos definidos en este estándar.

XSL es un lenguaje de hojas de estilo que, en combinación con XML, permite representar la información sin reescribir código y con diferentes formatos de salida.

Todos los terminales de comunicación inalámbricos presentan la mayor parte de las **restricciones** siguientes:

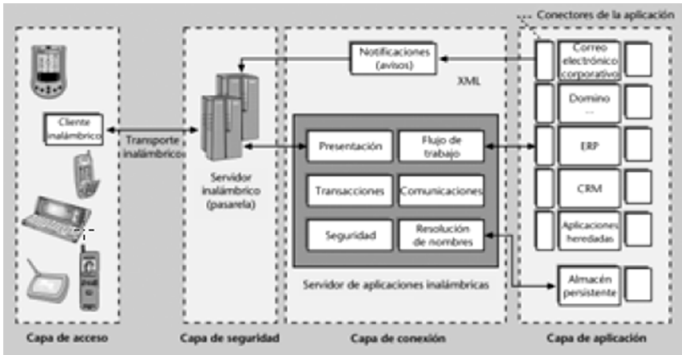
- Mecanismos de entrada de datos poco cómodos y especialmente lentos para la escritura de texto libre.
- Capacidad de procesamiento limitada, lo que implica eliminar gráficos y otros recursos multimedia complejos. Las aplicaciones deben diseñarse de manera que el procesamiento más pesado se realice en el servidor y no en el terminal cliente.
- Capacidad de almacenamiento limitada. Hay que procurar guardar los datos estrictamente necesarios.
- Dificultad para gestionar la memoria, un bien muy escaso. La capacidad de memoria es tan diminuta en comparación con la de un ordenador de sobremesa, que hay que utilizarla eficazmente sin acumular demasiados datos.
- Volatilidad de la información porque las baterías se han descargado, con posible pérdida de datos. Hay que diseñar políticas muy firmes de copias de seguridad o asegurarse de que el usuario no descargue la batería.

Respecto a la **pérdida de conectividad**, hay que decir que las aplicaciones deberían ser lo suficientemente robustas como para recuperarse de un corte de la conexión debido a la pérdida de cobertura. Una primera solución es la creación de aplicaciones clientes muy completas que incorporen la lógica del servidor necesaria para seguir trabajando fuera de línea mientras dure la pérdida de cobertura y que una vez recuperada, automáticamente se conecten y envíen los datos locales al servidor remoto, sin tener que empezar de nuevo y sin tener que reenviar la información.

Otra solución consiste en la implementación de colas de mensajes que se instalan en el servidor y recogen peticiones cuando el dispositivo inalámbrico no está conectado.

2. SERVICIOS CARACTERÍSTICOS DE LOS ENTORNOS MÓVILES

El middleware o software intermediario de comunicaciones inalámbricas es una denominación ambigua que abarca todo tipo de entornos, herramientas y servicios inalámbricos. Concretamente, comprende toda la tecnología situada por encima del sistema operativo y por debajo de las aplicaciones.



La arquitectura de una aplicación de un entorno de comunicación inalámbrica se puede describir según un modelo de cuatro capas, aunque la cantidad y el tipo de capas empleadas dependerán de la complejidad del problema.

La capa 1 o capa de acceso, describe el dispositivo inalámbrico desde el que el usuario accede a la aplicación. Las capas 2 y 3 engloban el middleware y los servicios que permiten que los datos y las aplicaciones de la capa 4 sean accesibles por medio de dispositivos inalámbricos. Finalmente la capa 4 o capa de aplicación, recoge todos los datos y aplicaciones corporativas accesibles desde la capa de acceso, como por ejemplo la mensajería electrónica, los datos de los clientes o las aplicaciones para el procesamiento de datos.

Las funcionalidades más críticas del **middleware** se reparten entre las capas 2 y 3 del modelo; en concreto la capa 2 o de seguridad, es la responsable de ofrecer una conectividad inalámbrica segura, optimizada y fiable. Los componentes principales de esta capa son las **pasarelas inalámbricas**. Estas pasarelas proporcionan las funcionalidades de conectividad por medio de las redes de comunicación inalámbrica, con independencia del modelo del terminal empleado o del operador contratado. En concreto, una pasarela de comunicaciones inalámbricas es la responsable de gestionar la conexión y la sesión de usuario por medio de dispositivos y de redes móviles. Otra responsabilidad fundamental de las pasarelas es la gestión de la seguridad en las comunicaciones mediante tecnologías de cifrado y autenticación.

Los **servidores de aplicaciones** de comunicaciones inalámbricas son una extensión natural de los servidores de aplicaciones para dar apoyo a los dispositivos inalámbricos. Deben ser independientes de los dispositivos y de las redes de acceso. Los **transcoders** son una pieza de la capa 3 que procesa contenidos y los presenta con un nuevo formato más adecuado a las características del dispositivo y la red desde los que accederá. Esta transformación suele ser dinámica y parte tanto de contenidos estáticos como de contenidos generados dinámicamente.

El **portal multimedia inalámbrico** se orienta al usuario final con el objetivo de reflejar sus necesidades de acceso seguro y robusto en ubicaciones y circunstancias cambiantes. Un portal de estas características ha de garantizar una serie de servicios mínimos:

- Agregación e integración de información relevante teniendo en cuenta el perfil del usuario.
- Formateo dinámico de la información según las características de los terminales y redes soportados.
- Presentación de la información teniendo en cuenta posibles cambios en el terminal o en la red.
- Actualización dinámica: con información como bolsa de valores, noticias, etc.

Los **servicios móviles de localización** proporcionan un servicio personalizado y contextualizado según quién, cuándo y desde dónde se soliciten. La diferencia entre localización y posición consiste en el nivel de detalle empleado: localización es un término genérico que puede tener en cuenta grandes extensiones geográficas, mientras que posición es la información exacta sobre la localización de alguien. Esta información sobre localización/posición de un individuo no tiene valor por sí misma. Requiere aplicaciones y servicios que la exploten en un momento determinado en función del perfil del usuario.

Los servicios y las aplicaciones basados en la localización son visibles para el usuario, pudiendo obtener o deducir, interpretar y utilizar la información sobre su posición: páginas amarillas, predicción del tiempo, información del tráfico…

Los servicios y aplicaciones sensibles a la localización, los activa directamente el usuario cuando entra en un área determinada, previo consentimiento o

subscripción. Aquí se incluyen los servicios de marketing directo, como los cupones instantáneos definidos como ofertas emitidas por establecimientos cercanos a la localización del usuario en un momento dado.

Se pueden distinguir cuatro tipos de técnicas básicas para la determinación de la posición:

- Técnicas basadas en el terminal, por ejemplo el GPS, en el que el terminal de manera autónoma calcula su posición. SU exactitud es de 5-10 metros para objetos estáticos y de 10-100 metros para objetos en movimiento.
- Técnicas basadas en la red, en las que la red de comunicaciones calcula la posición de manera también autónoma. Por ejemplo la identificación de celda (Cell-ID) funciona sobre redes GSM, GPRS y WCDMA; es el mecanismo más sencillo para describir la localización de un individuo: simplemente proporciona la localización de la antena o estación base que en un momento dado provee el teléfono móvil en cuestión del servicio de conectividad. El área geográfica cubierta por una determinada estación se denomina celda; así pues la exactitud de la técnica depende del tamaño de las celdas, cuyo diámetro puede varias desde los 500 metros hasta los 20 kms. La estrategia típica para mejorar la exactitud consiste en reducir el tamaño de las celdas. En las ciudades, las redes de estaciones son más densas y tienen celdas más pequeñas. En cambio, en las zonas rurales hay menos antenas, por tanto la exactitud de este servicio será poco precisa.
- Técnicas asistidas por el terminal (por ejemplo E-OTD) en las que éste da asistencia a la red de comunicaciones que finalmente calcula la posición. Se basa en la detección, por parte del terminal móvil de la diferencia de tiempo de llegada de las señales procedentes de las diversas estaciones base que le dan servicio (GSM y GPRS). La posición del terminal móvil se determina a partir de los componentes geométricos correspondientes a los retrasos temporales entre el terminal móvil y las estaciones base. Su exactitud oscila entre 100 y 500 metros.
- Técnicas asistidas por la red: (A-GPS) en las que la red de comunicaciones da asistencia al terminal, que finalmente calcula la posición.

Avisos y tecnología push

En un modelo cliente-servidor clásico, los clientes solicitan un servicio o una información al servidor que responde a la petición. Esto se denomina tecnología pull: el cliente extrae información del servidor. La tecnología push también se basa en un modelo cliente-servidor, pero no hay una petición explícita por parte del cliente antes de que el servidor transmita la información o el servicio. Otra manera de expresarlo es que mientras que en las transacciones de tipo pull el cliente siempre inicia el flujo de información, en las transacciones push es el servidor el que inicia el flujo de información.

El **SMS** (Short Message Service) es un ejemplo de tecnología push e identifica el servicio de mensajería que posibilita el envío de mensajes de texto corto entre terminales móviles y que se basa en el protocolo SMPP (Short message peer to peer), un protocolo de mensajería abierto y diseñado para simplificar la integración de aplicaciones de datos con redes de dispositivos móviles inalámbricos como el GSM.

Es importante tener en cuenta que el éxito de cualquier tecnología o servicio ha de medirse no sólo en términos de velocidad, capacidad de transmisión y seguridad, sino también en términos de utilización. En el caso del SMS, el éxito ha superado las expectativas de cualquier operador de telefonía: se ha convertido en el sistema de comunicación de toda una generación.

La posibilidad de que el terminal destinatario del mensaje esté inactivo o sin cobertura hace necesaria la existencia de entidades destinadas al almacenamiento de los mensajes que no pueden ser entregados a sus destinatarios. El BSC (Base station center) se encarga de transmitir el mensaje que procede de un terminal móvil dentro del área de cobertura de una antena hacia la entidad que almacena los mensajes, el SMSC (Short messaging service center). Si

el terminal móvil receptor no está disponible o está desconectado en ese momento, el mensaje se almacenará en el SMSC y se volverá a enviar posteriormente. El mensaje quedará en el SMSC hasta que se consiga el envío o se llegue al máximo de tiempo de validez, el periodo máximo que un mensaje se puede almacenar en un SMSC.

El **EMS** (enhanced messaging service) es una evolución del SMS basada en un diseño inicial de Ericsson aceptado por el 3GPP, que permite el envío a otro usuario de una combinación de imágenes, texto con formato, melodías, sonidos y animaciones. Este servicio no comporta ningún cambio para los centros SMS de mensajería, ya que el envío es transparente para estos centros y el único requerimiento para la correcta visualización del mensaje es que el terminal móvil soporte las especificaciones de este tipo de mensajería. Para los envíos de gran tamaño el mensaje resultante puede utilizar la práctica totalidad del tamaño máximo de un mensaje SMS; en estos casos y para permitir el envío de más información, se puede utilizar el mecanismo de concatenación de mensajes que incorpora el protocolo SMPP. El estándar SMS permite la concatenación de un total de 255 mensajes de 140 bytes cada uno, para obtener un único mensaje de aproximadamente 38 Kbs. Pero los terminales móviles actuales sólo soportan la concatenación de entre 3 y 6 mensajes, pues las concatenaciones de tamaño superior se considerarán mensajes separados.

El **MMS** (Multimedia messaging service) permite el envío de mensajes con una combinación de uno o más de los siguientes componentes: texto alfanumérico, imágenes, sonidos, animaciones y video. Este sistema comporta unos cambios fundamentales en la mensajería, no sólo en lo tocante al tipo de mensajes que se pueden enviar y a los mecanismos utilizados para enviarlos y recibirlos, sino también en lo que respecta a la infraestructura de red necesaria para poder enviarlos. El SMS utiliza para la emisión y la recepción de mensajes el canal de señalización de las redes GSM, lo cual permite la recepción de mensajes mientras se hace, por ejemplo, una llamada de voz. Sin embargo, este hecho limita el formato de los mensajes que pueden ser enviados por SMS, ya que el canal de señalización tiene un ancho de banda pequeño.

El MMS difiere del SMS porque aprovecha la gran capacidad de las redes de tercera generación para enviar los mensajes por el canal de transmisión de datos. De este modo, no tiene limitación de ancho de banda y, al mismo tiempo, utiliza protocolos estándar de internet para enviar y recibir esa información.

Para prever el éxito de penetración en el mercado de todas estas nuevas tecnologías de comunicación, hay que tener en cuenta factores muy importantes, como la evolución de las redes actualmente existentes en las fechas previstas y la presencia en el mercado de una elevada cantidad de terminales compatibles con estas tecnologías. Además, cuando la aplicación de una tecnología conlleva un cambio de terminal, el éxito de implantación también dependerá de la decisión del usuario de invertir o no en ese nuevo terminal móvil.

Portales de voz

Estos portales son webs que permiten el acceso y la navegación por su información desde un terminal telefónico mediante la voz. De manera análoga a los portales de internet, los portales de voz permiten una interacción entre los usuarios y el servidor de contenidos.

Existen dos tecnologías del habla claves en la interacción persona máquina: el reconocimiento de voz y la conversión de texto a habla. El primero (traduce palabras habladas en palabras escritas) puede tener dos utilidades principales: el dictado (puede crearse con la voz una pieza de texto) y la navegación (cuando se utiliza la voz para controlar el sistema).La conversión de texto a voz aumenta la creación de sonidos a partir de palabras escritas.

El **voiceXML** es un lenguaje basado en XML y definido por el W3C que permite diseñar diálogos orales para acceder a la web mediante la voz con teléfonos móviles.

TEMA 4 ENTORNOS DE DESARROLLO

La gran variedad de dispositivos móviles provoca la continua aparición de nuevos estándares y lenguajes de programación. A medida que los navegadores de estos dispositivos son capaces de procesar diferentes formatos de contenido, la oferta crece más y más, dificultando el desarrollo de software en entornos de comunicación inalámbrica.

Podemos distinguir y clasificar los entornos de desarrollo según los dispositivos a los que van dirigidos:

- Entornos independientes de los dispositivos: Son los que permiten desarrollar software apto para cualquier tipo de dispositivo, sin basarse en las funcionalidades y características específicas del sistema operativo y del hardware.
- Entornos dependientes de los dispositivos: Son los que permiten explotar a fondo las posibilidades del sistema operativo y del hardware empleados, siempre que la tipología de los dispositivos clientes sea reducida y previsible. La lista de posibilidades es realmente extensa y creciente.

Los entornos de desarrollo contienen emuladores que simulan la ejecución de código en dispositivos concretos. Hay infinidad de emuladores, pero es preciso tener en cuenta que el comportamiento del software en el emulador no necesariamente ha de coincidir exactamente con el que tendrá en el dispositivo real. Los emuladores facilitan un primer nivel de depuración del código; se requiere una segunda depuración con los dispositivos físicos.

1. ENTORNOS DEPENDIENTES DEL DISPOSITIVO

Web Clipping de Palm OS

Una aplicación web clipping es un conjunto de páginas HTML comprimidas con un formato denominado PQA (Palm query apllication), diseñado para reducir los requerimientos de ancho de banda y de pantalla necesarios para ser mostrados al usuario. El PQA es un subconjunto del HTML.

La navegación web clipping no se basa en un modelo de hiperenlaces, sino en preguntas-respuesta entre el usuario y el servidor intermediario.

Entornos visuales de Pocket PC y Windows CE

Estos entornos visuales permiten desarrollar, depurar y emular rápidamente aplicaciones móviles para plataformas Pocket PC y Windows CE. Todo ello empleando dos lenguajes de programación bastante maduros en el mercado: Visual Basic y Visual C++. Pese a esa madurez, para cada tipo de dispositivo se requiere un SDK diferente para compilar y ejecutar la aplicación.

Con el eMbedded Visual Basic y el eMbedded Visual C++ se pueden crear componentes y aplicaciones con interfaz gráfica que se ejecutarán por encima de las funcionalidades nativas de los dispositivos, pero no implementarán drivers ni servicios de bajo nivel.

2. ENTORNOS INDEPENDIENTES DEL DISPOSITIVO

WML

La estructura del WML se define mediante el XML y el correspondiente DTD. Si se genera un documento WML, siguiendo las especificaciones del XML, decimos que se está formateando correctamente y cuando el documento cumple con las especificaciones de su DTD, decimos que es válido. Los documentos creados con el WML se componen de unas unidades mínimas de información,

cartas, que se estructuran en barajas, de manera similar a como los documentos HTML se componen de diferentes marcos de información.

Las aplicaciones diseñadas con el WML permiten al micronavegador que incorporan los terminales móviles navegar de manera sencilla hacia la carta anterior o posterior de uno o más documentos. Cuando se navega por un contenido, el navegador guarda en su memoria toda la baraja, pero sólo muestra una carta al usuario: así, la navegación hacia otra carta no comporta un nuevo acceso a la red, lo cual disminuye el tiempo de respuesta y reduce el consumo de batería y procesador.

Personal Java y JavaPhone

Combinado con la plataforma Personal Java, el API JavaPhone proporciona el entorno ideal para una entrega de información fiable y dinámica a dispositivos de telefonía. Esta nueva API se diseñó para proveer de acceso a las funcionalidades más características de los teléfonos móviles más sofisticados y de pantallas de teléfono con acceso a internet.

El secreto para poder ejecutar el Java en dispositivos limitados es la reducción del tamaño de las clases que se instalan en el entorno de ejecución. La versión Micro Edition elimina todas las clases innecesarias quedándose solamente con las que forman el núcleo básico para la ejecución de aplicaciones sobre dispositivos móviles y reduce estas clases eliminando todas sus funciones y procedimientos redundantes y duplicados.

TEMA 5 SEGURIDAD EN COMUNICACIONES INALÁMBRICAS

1. LA PROBLEMÁTICA DE LA SEGURIDAD

Los cuatro conceptos clave de seguridad de la información son:

- **Confidencialidad**: Propiedad que asegura que sólo tienen acceso a la información los que están autorizados (privacidad).
- **Integridad**: Asegura la no alternación de la información (inserción, borrado o sustitución de la misma).
- **Autenticación**: Hace referencia a la identificación, es el nexo de unión entra la información y su emisor.
- **No repudio**: Asegura que ninguna parte pueda negar ningún compromiso o acción tomados anteriormente

La preocupación por la seguridad en los entornos inalámbricos es creciente, ya que su uso para aplicaciones de comercio electrónico requiere un alto grado de seguridad. Cuando hablamos de técnicas para prevenir la seguridad podemos hacer una distinción clara entre las que trabajan en el nivel físico de la comunicación y las que trabajan en el resto de niveles, tanto en el de enlace como el de aplicación.

Entre las técnicas habituales en el nivel físico hallamos las de **difusión de espectro**, que basan su funcionamiento en fraccionar la señal de radio y transmitirla de manera imperceptible por diferentes frecuencias: al no conocerse la manera en que se ha distribuido la señal por las diferentes frecuencias, no se puede reconstruir, ya que las distintas señales que se reciben en cada frecuencia, aisladamente son percibidas como ruido.

2. TECNOLOGÍAS DE CORTO ALCANCE: BLUETOOTH

A la hora de estudiar la seguridad de las tecnologías de corto alcance, nos centraremos en la tecnología de Bluetooth, ya que las tecnologías DECT y HomeRF son propietarias y un porcentaje mínimo de su información es pública.

Los dispositivos Bluetooth operan en tres modos de seguridad: Modo de seguridad 1, modo 2 y 3.

El **modo de seguridad 1** no incorpora ningún mecanismo de seguridad, permitiendo la conexión entre cualquier dispositivo y/o aplicación. De hecho, no tendría que considerarse de seguridad, pero las especificaciones de la arquitectura así nos lo indican.

El **modo de seguridad 2** ofrece una seguridad débil, es el llamado nivel de servicio, porque las restricciones se aplican cuando la comunicación entre los dispositivos ya se ha efectuado. Pese a ello, se utiliza mucho porque si se restringen las conexiones a nivel de enlace no es posible diseñar aplicaciones más abiertas, como el intercambio de tarjetas de negocio o la consulta de los servicios ofrecidos por un dispositivo. La política de seguridad en estos casos se basa en la información almacenada en dos bases de datos: la de dispositivos y la de servicios.

La base de datos de dispositivos mantiene información de los requisitos de seguridad de los dispositivos de acuerdo con la confianza que se tiene en ellos. Se especifican dos niveles de confianza:

- Dispositivos de confianza: Han sido autenticados previamente, tienen una clave de enlace almacenada y en la base de datos están marcados como dispositivos de confianza.
- Dispositivos untrusted: Autenticados también previamente, tienen una clave de enlace almacenada pero se aplican como de no confianza normalmente porque no se tiene con ellos una relación permanente.

Por otro lado, la base de datos de servicios especifica las necesidades de seguridad de los distintos servicios: abiertos, con autorización o con autenticación y autorización.

El **modo de seguridad 3** en el nivel de enlace es el sistema más seguro especificado en la arquitectura Bluetooth, ya que las restricciones de seguridad se aplican antes de la conexión entre los dispositivos, así se minimiza el riesgo de ataques de dispositivos ya conectados.

El proceso de autenticación es de tipo reto-respuesta y requiere que los dos interlocutores conozcan un valor con anterioridad al proceso, que en este caso es la llamada clave de enlace.

Aunque la arquitectura Bluetooth incorpora ciertos niveles de seguridad, existen puntos del diseño poco robustos:

- En el caso de no haberse dado una conexión previa entre los dispositivos, la clave de enlace se obtiene por medio de la clave de inicialización. Esta clave se genera, básicamente, a partir del PIN, ya que el valor aleatorio se transmite en claro de un dispositivo a otro. Teniendo en cuenta que los PIN están formados por 4 dígitos, el número de posibilidades es bastante bajo.
- Aún es peor si se utiliza la clave de dispositivo como clave de enlace. La clave de dispositivo se general al inicializarse el dispositivo y raramente se cambia. Eso hace que cuando un dispositivo A ha usado su clave de dispositivo como clave de enlace para autenticarse ante B, el siguiente proceso de autenticación de A ante un tercer dispositivo con su clave de dispositivo como clave de enlace no sea fiable: el dispositivo B podría hacerse pasar por A dado que conoce su clave de dispositivo.

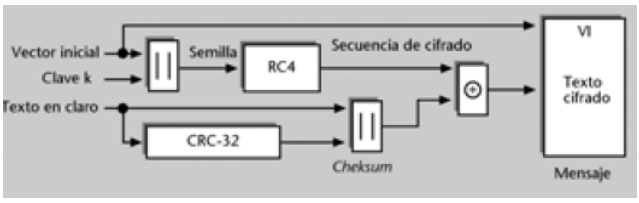
Para finalizar, cabe destacar que los esquemas de seguridad que incorpora la arquitectura Bluetooth autentican dispositivos, pero no usuarios. Eso, junto con la poca longitud del PIN, hace que no sea adecuado para ciertas aplicaciones.

3. EL ESTÁNDAR IEEE 802.11

En el estándar IEEE 802.11 se especifican dos servicios de seguridad: uno para obtener la propiedad de autenticación y el otro para la propiedad de confidencialidad e integridad.

El **servicio de confidencialidad** del estándar IEEE 802.11 se basa en el algoritmo WEP. Este algoritmo proporciona las propiedades de confidencialidad e integridad. La confidencialidad se logra utilizando criptografía de clave simétrica, en particular el cifrador en flujo RC4. La integridad se obtiene mediante un ckecksum CRC32. Tal como dice el estándar, el algoritmo WEP pretende dotar a las redes inalámbricas de las mismas propiedades de seguridad que las redes con cables. Este argumento ha sido utilizado a menudo para rebatir los problemas de debilidad del algoritmo, ya que muchos de esos problemas también están en las redes con cables.

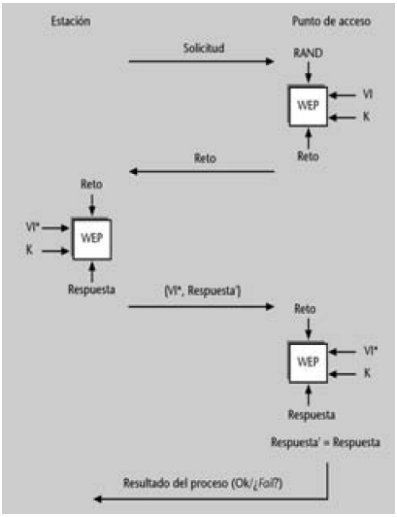
El proceso de descifrado de la información que lleva a cabo el receptor es exactamente el inverso al de cifrado que reproducimos en la imagen lateral.



Como el RC4 es un criptosistema de clave compartida, la estación y el punto de acceso necesitan intercambiar tanto el vector inicial VI como la clave K para poder comunicarse utilizando el WEP. Como el VI se envía en claro, la seguridad del algoritmo depende solamente de la clave. Aún así, hay que asegurar la integridad de la transmisión del VI, ya que si el VI utilizado por el emisor no es exactamente igual que el del receptor, los procesos de cifrado y descifrado no serán inversos. Este intercambio de información se realiza durante el proceso de autenticación.

Sobre el **proceso de autenticación** diremos que el estándar IEEE 802.11 tiene dos variantes: el OSA y el SKA. OSA es la implementación obligada en el estándar y lo incluyen por defecto la mayoría de los productos que se pueden encontrar en el mercado. Como su nombre indica (Open System Autenthication), es un sistema de autenticación abierto y que, por lo tanto, no limita el acceso, cosa que implica que, desde el punto de vista de la seguridad, este sistema por sí mismo no tiene interés.

El método SKA (Shared Key Autenthication) permite la autenticación de las estaciones y los puntos de acceso por medio del algoritmo WEP, junto con un sistema de reto-respuesta. Este proceso de autenticación consiste en el intercambio de 4 mensajes entre la estación que se autentica y el punto de acceso. El sistema de intercambio de claves no implica el envío de claves en claro, pero requiere que la clave secreta compartida haya sido proporcionada por un canal seguro con anterioridad al proceso de autenticación.



El punto de acceso envía continuamente una señal de baliza para anunciar su presencia. Una estación que quiera acceder a la red, al encontrar la señal de baliza, inicia el proceso de autenticación con el punto de acceso cuya dirección figura en la señal de baliza.

El proceso de intercambio de mensajes es el siguiente:

- La estación envía un mensaje al punto de acceso para solicitar la autenticación.
- El punto de acceso genera un reto de 128 bytes utilizando el algoritmo WEP a partir de un valor pseudoaleatorio, una clave K y un vector inicial VI.
- La estación genera la respuesta utilizando el algoritmo WEP con el valor reto, la calve K y un VI diferente del que se ha usado en el paso anterior.
- El punto de acceso calcula la respuesta utilizando el algoritmo WEP con la clave compartida, el valor reto y el valor VI recibido de la estación. Si ambas respuestas coinciden, la estación ha sido autenticada correctamente.

El diseño y el funcionamiento de las redes de área local hacen que la captura del tráfico de red sea simple, utilizando una tarjeta de red en modo promiscuo (que acepta todos los mensajes que le llegan). Si a esto le añadimos el hecho de que en las comunicaciones inalámbricas no se necesita estar conectado a la red para recibir la señal, tenemos que es relativamente fácil realizar un ataque sobre las mismas.

Uno de los problemas añadidos que encontramos en el proceso de autenticación es que el estándar sólo obliga a implementar el modelo OSA, así que en muchos productos sólo viene este modelo y cualquier estación que sea capaz de generar tramas correctas se puede autenticar.

Pero el proceso de autenticación SKA tampoco está libre de problemas, uno de los principales es la longitud de la clave: el estándar fija en 40 bits esta longitud, y esto hace que sea lo suficientemente pequeña como para poder intentarse un ataque de "fuerza bruta", es decir, probando todas las combinaciones posibles. Este hecho deriva de un problema legal en EEUU. Cuando se fijó este estándar una ley prohibía la exportación de EEUU de criptografía fuerte (con claves de longitud grande), ya que consideraban esto como armamento. Por ello, muchos estándares que incorporan esquemas criptográficos utilizan, como máximo, claves de 40 bits. En la actualidad esta ley ya no está en vigor, pero se siguen sufriendo sus consecuencias, como en este caso.

Las **recomendaciones** de seguridad para el estándar actual son:

- Situar la red inalámbrica fuera del perímetro de acción del firewall de la empresa y nunca en la red de la organización.
- Utilizar redes privadas virtuales para el acceso entre estaciones móviles de red inalámbrica y estaciones en el firewall de la empresa.
- Eliminar las rutas que permiten el acceso a internet por la red inalámbrica.

- Tener una buena política de gestión de claves para que cada estación tenga una clave de cifrado diferente y que estas claves se actualicen con frecuencia.

4. LAS TECNOLOGÍAS DE GRAN ALCANCE: GPRS

Nos vamos a centrar en el GPRS dado que esta tecnología se puede considerar como un servicio sobre GSM, y muchos de los procedimientos y algoritmos de seguridad se basan en los mismos principios.

El **proceso de autenticación** de un terminal en una red GPRS, al igual que sucede en las redes GSM, utiliza un modelo reto-respuesta. Los mayores problemas en la seguridad del sistema GPRS y también del GSM, recaen en el hecho de que utilizan sistemas propietarios, lo que dificulta su evaluación por parte de la comunidad científica internacional. Así, no se puede asegurar que los algoritmos sean lo suficientemente robustos para seguir siendo seguros en el caso de que la descripción del algoritmo se hiciera pública.

Por otro lado, el proceso de autenticación se basa en la clave que comparten el terminal y la operadora. Esta clave figura en la tarjeta SIM del usuario. Eso comporta que la clonación de esta tarjeta implica la duplicación de la identidad del usuario y, por tanto, todo el gasto que se realice con la tarjeta clonada se facturará al usuario legítimo.

Texto elaborado a partir de:
Comunicaciones inalámbricas
Josep Prieto Blázquez, Genís Berbel Navarro, José Manuel Santos Villa, Silvia González González, Jordi Herrera Joancomartí
Febrero 2008