Comunicaciones Móviles

GSM

Jesús Sanz Marcos

e-mail: jesus.sanz@upcnet.es

Barcelona, Spain. Jan 2002

Planes de frecuencia

- enlace ascendente (móvil-base) 890-915 MHz
- enlace descendente (base-móvil) 935-960 MHz
- sistema duplex con espaciado entre canales de: 45 MHz
- ancho de banda de cada radiocanal: 200 kHz
- 125 radiocanales bidireccionales disponibles
- tipo de modulación: GMSK diferencial (MSK con pulso de conformación gaussiano)
- sistema limitado por interferencias (1er nulo a 0.75 R_b = 200 kHz)
- velocidad de transmisión: 270,8 kbps

Estructura jerárquica

- **hipertrama**: 3h 28 min 53 s 760 ms (2048 multitramas)
- **supetrama**: 6.12 s (contiene o 51 multitramas o 26 multitramas)
- **multitrama**: 120 ms si tiene 26 tramas
- **multitrama**: 235 ms si tiene 51 tramas
- **trama**: 4.615 ms (8 time slots)
- **time slot**: 546.12 μs

Rágafas

- **Normal**: T(3) Coded data (57) S(1) Entrenamiento(26) S(1) Coded data (57) TB(3) BG(8.25)

  - 148 bits en total (546.12 μs)
  - T(Tail Bits) sirven para inicializar al igualador.
  - S(Stealing Flag) indica si la ráfaga transporta información de control urgente en lugar de información de usuario.
  - Secuencia de entrenamiento para estimar la respuesta impulsional y seguimiento Time Advance (TA).
  - Periodo de guarda de 8.25 bits (31.4 μs) aproximadamente igual al transitorio de potencia.
  - $\frac{148\ \text{bits} + 8.25\ \text{bits}}{576.9ms} = 270.8\ \text{kbps}$

- **Sincronización**: T(3) Coded data (39) Entrenamiento(64) Coded data (39) TB(3) BG(8.25)

  - 148 bits en total (546.12 μs)
  - primera ráfaga que detecta el sistema.
  - Secuencia de entrenamiento es única para el sistema y es de mayor duración (para facilitar el sincronismo).
  - Los bits codificados contiene el identificador de la estación base (BSIC) y los identificadores de Multitrama y de supertrama para sincronización.

- **Correción de frecuencia**: T(3) Secuencia todo “0” (142) TB(3) BG(8.25)

  - 148 bits en total (546.12 μs)
  - transmite un tono puro desplazado de la frecuencia portadora a 67.7 KHz ($R_b/4$)
  - permite encontrar y demodular la ráfaga de sincronización temporal del sistema.
  - Permite la sincronización del móvil al reloj maestro del sistema.

• **Acceso**: T(8) Sincronización (41) Coded Data (36) TB(3) BG(60 bits) BG(8.25)

- 148-60 bits en total (546.12 μs)
- elevado tiempo de guarda para evitar colisiones con otras ráfagas)
- (60+8.25) bits equivalen a 0,252 ms, 38.2 km y 35.5 km es el radio máximo de la celda.
- Acceso según protocolo ALOHA.
- Power Ramping aproximadamente de 30 μs
- Tolerancia de 2dB durante la transmisión de la ráfaga.
- TA (Time Advance) = $2T_{propagación} = 2T_p$
- Máxima resolucón en tiempo = 3.7 μs = T_b^{-1}
- Distancia de resolución = $\frac{T_b c}{2} = 550\,m$
- $TA \in \{0..63\}$
- Tiempo de incertidumbre máximo en la recepción del burst de acceso en la base = $T_i = 2T_p = 233\,ms = 63$ bits

Canales lógicos

• son combinaciones ordenadas de rágafas dentro de una estructura de trama.
• existen canales lógicos de **TRÁFICO** y de **CONTROL**.

• canales lógicos de **tráfico**: transmiten información generada por el usuario (voz y/o datos)
- TCH/HS (*Traffic Channel Half-Rate Speech*) ~ Rafaga Normal
- TCH/FS (*Traffic Channel Full-Rate Speech*) ~ Rafaga Normal
- TCH/F9.6, TCH/F4.8, TCH/F2.4 (*Traffic Channel Full-Rate Data*) ~ Rafaga Normal
- TCH/H4.8, TCH/H2.4 (*Traffic Channel Half-Rate Data*) ~ Rafaga Normal

• canales lógicos de **control** (**radiodifusión**): proporcionan al móvil información suficiente para su sincronización con la red.
- BCCH (*Broadcast Control channel*): se utiliza para informar al móvil de los parámetros del sistema necesarios para identificar la red y acceder a la misma. ~ Rafaga Normal
- FCCH (*Frequency Correction Channel*): Informa al móvil de la frecuencia portadora de la estación base. Permite la sintonía de los receptores móviles. ~ Rafaga de Corección de Frecuencia.
- SCH (*Synchronization Channel*): permite identificar la estación base sintonizada y sincronizarse con la estructura de trama. Informa al móvil de la secuencia de entrenamiento que utiliza la base y que es necesaria para la demodulación de la ráfaga ~ Rafaga de Sincronización.

• canales lógicos de **control** (**dedicados**): se utilizan para transmitir información de control entre la red y el móvil, o incluso entre los propios transceptores.
- SACCH (*Slow Associated Control Channel*): transmite información dedicada al mantenimiento del enlace. Se utiliza siempre asociado a un canal de tráfico. En el enlace descendente se envía el Time Advance y la potencia a transmitir y en el enlace ascedentente las medidas realizadas por el móvil para el Handover. Se transporta concatenando slots 13 ~ Rafaga Normal
- FACCH (*Fast Associated Control Channel*): reemplaza a un canal de tráfico y sirve para transmitir informaciones de control urgentes. ~ Rafaga Normal
- SDCCH (*Stand-alone Dedicated Control Channel*): se utiliza para intercambiar mensajes entre el móvil y la base, una vez el móvil ha accedido a un slot y antes de establecer la comunicación. ~ Rafaga Normal

• canales lógicos de **control** (**comunes**): permiten establecimiento del enlace entre el móvil y la base. Se transmiten en el slot 0 de una multitrama de 51 tramas.
- RACH (*Random Access Channel*): se utiliza por el móvil para realizar una petición de llamada. ~ Rafaga de acceso.
- PCH (*Paging Channel*): avisa al móvil de las llamdas entrantes procedenrtes de la estación base. ~ Rafaga Normal
- AGCH (*Access Grant Channel*): concede o niega la llamada solicitada por el móvil. En caso de concesión de llamada también informa del valor del Time Advance. ~ Rafaga Normal

- comentarios:
  - En TDMA no es necesario transmitir y recibir señales al mismo tiempo. Es decir, el móvil no necesita un duplexor. Los slots de desalineamiento se utilizan para acomodar el tiempo de conmutación del sintetizador necesario para saltar 45 MHz.
  - El móvil puede usar parte del tiempo en que no transmite para medir la potencia proveniente de bases vecinas. Pero necesita más tiempo para identificar (detectar y presincronizar) las bases vecinas. Para ello se utiliza la trama IDLE de la multitrama de 26 tramas.

  - CCH (Broadcast Control channel): se utiliza para informar al móvil de los parámetros del sistema necesarios para identificar la red y acceder a la misma. ~ Rafaga Normal

FCCH (Frequency Correction Channel): Informa al móvil de la frecuencia portadora de la estación

  - TCH/HS (Traffic Channel Half-Rate Speech) ~ Rafaga Normal
  - TCH/FS (Traffic Channel Full-Rate Speech)

Señales vocales, codificación y entrelazado

- cada 20 ms el VOCODER proporciona 260 bits (13 kbps): 50(Ia) de alta importancia, 132 normales (Ib) y 78 bits que añaeden calidad (Ic).
- los bits más importantes se protegen utilizando códigos correctores de errores.

$$convolucional_{r=\frac{1}{2},K=5}\left(\left(Ia_{50}+CRC_3\right)+Ib_{132}+4_{"0"}\right)+Ic_{78}=456\text{ bits}$$

- una ráfaga transporta 114 bits. Puesto que hay 8 rágafas por trama (4.51 ms) la velocidad de datos en el canal (*Channel Bit Rate*) es de $\frac{114\text{ bits}}{4.61ms}=24.7\text{ kbps}$
- los 456 bits se repartan y entrelazan considerando 8 rágafas consecutivas a razón de 57 bits por ráfaga. Cada ráfaga contiene la contribución de dos bloques consecutivos de voz codificada.

- capacidad del SACCH. Si el *throughput* real para el canal de tráfico es de 24.7 kbps y dentro de una multitrama de 26 tramas se utilizan 24 tramas para voz (22.8kbps) y 1 para el SACCH tenemos que el *throughtput* real para este canal es 24.7kbps/26=950 bps sin codificación y con codificación tenemos 382 bps.

- codificación del canal de datos a 9.6 kbps:

$$punturing_{\text{1 de cada 16 bits se elimina}}\left(convolucional_{r=\frac{1}{2},K=5}\left(9.6\text{kbps}\cdot 20ms=240\text{bits}+4_{"0"}\right)\right)=456$$

- codificación del canal de señalización: PCH, SDCCH, BCCH, SDCCH:

$$convolucional_{r=\frac{1}{2}}\left(\text{código FIRE}_{+\text{40 bits de paridad}}\left(184\text{ bits de señalización}\right)+4_{"0"}\right)$$

Estructura de la red GSM

- **BTS** (*Base Tranceptor Station*): realiza los procesos de TX-RX y procesado de la señal recibida. Cada BTS puede tener entre 1 y 16 radiocanales asignados. Forma el multiplex GSM, realiza medidas de la señal radio proveniente del móvil, establece el enlace radio con el usuario móvil (modulación, demodulación, igualación, codificación, etc). Gestión del time–advance, control de potencia, operación y mantenimiento.

- **BSC** (*Base Station Controller*): constituye el primer nivel de concentración de tráfico hacia la red con objetivo de minimizar costes de transmisión. Gestiona y controla las BTS, responsable de la asignación y liberación de radioncanales con el móvil y de canales terrestres con la red. Fija el contenido de los canales de radiodifusión y asigna los mensajes de paging. Gestiona los procesos de transferencia Handover bajo su control. Ejecuta los algoritmos de gestión de potencia y cifrado.

- **MSC** (*Mobile Switching Center*): es una central de conmutación ISDN responsable del control de llamada: establecimiento, mantenimiento y liberación de una comunicación. El GMSC es el interfaz de la red fija con la red móvil. Sus funciones son las de enrutado de las llamdas hacia/desde el exterior (PSTN, ISDN)

desde/hacia un móvil y de la facturaicón. Controla varias BSC y puede conectarse con diversas redes de telecomunicación. Responsable de la gestión de movilidad (localización y autentificación) en conjunto con HLR y VLR. Handover entre distintas BSC.

• **HLR** (Registro localización del abonado): es una base de datos que almecen la identidad y los datos de los usuarios abonados, independientemente de la localización real de los mismos en un determinado momento. Proporciona los datos necesarios al GMSC para localizar al móvil cuando se desea establecer una llamada dirigida hacia éste.

- MSISDN : número telefónico para llamarle desde la red pública.
- IMSI: international mobile susbcriber identity.
- Datos de localización de la VLR: LMSI (puntero, númeor de registro o expediente asociado a un abonado).
- VLRID: identificador de las distintas VLR.
- Tripletas de autentificación: SRES, Kc y RAND.

• **VLR** (Registro de localización visitante): es una base de datos controlada por la MSC que contiene toda la información relevante de los terminales móviles que en un momento estan en el área de localización controalda por el VLR. Realiza en la MSC la autentificación del móvil. Actua como caché del HLR. Usualmente está incorporado al MSC o GMSC del que forma parte y se conecta con otros VLR y HLR a través del sistema de señalización SS7.

• **AUC** (Centro de autentificación): gestiona los datos de seguridad y autentificación de los abonados. Proporciona al HLR los valores de (RAND,RED y Kc) que permiten la autentificación del móvil en cada MSC/VLR.

• **EIR** (Registro Identificación de Equipos): es una base de datos mundial, contiene listas con números de serie de equipos móviles que debido a algún defecto o porque han sido robados no deben acceder a la red. Contiene otra con los valores del IMEI (International Mobile Equipment) permitidos.

• **SMSC** (Centro del servicio de mensajería): es independiente de la red GSM. Permite enviar y recibir mensajes cortos (140 caracteres) desde o hacia otros terminales móviles utilizando las portadoras de señalización GSM y puede establecer conexión con otros sistema sde correo elect´ronico. La transmisión de un mensaje corto se puede producir incluso simultáneamente con una transmisión de voz. Es una comunicación en una sola direcicón.

• Tarjetas **SIM** (Subscriber Identity Module): permite personalizar el terminal móvil. En ella residen todos los parámetros identificativos del usuario junto con los tipos de servicio contratados. Además también contiene los números de seguridad para evitar usos fraudulentos del terminal móvil: PIN (Personal Identification Number), PUK (PIN Unblocking Key), IMSI (International Mobile Subscriber Identity), Ki: clave para la autentificación. Existen dos versiones SIM: una del tamaño de una tarjeta de crédito y otra plug-in (15mmx25mm) para móviles de tamaño reducido.

Planos funcionales del sistema

• **Transmisión**: suministra todos los enlaces físicos para el transporte de la información de usuario y de señaliación. Transporte desde la BTS a la MS (líneas alquilidas de 2Mbps, enlaces de microondas, representan más del 30% de los costes de operación de toda la red móvil). Sistema TDMA con multiplexado en frecuencia. Celdas de agrupación (7 o 9 para antenas omnidireccionales) y (4 o 7 para antenas sectoriales de 120º). Portadores por celda (entre 1 y 7 para antenas omnidireccionales, entre 7 y 20 para antenas sectoriales, una BTS opera con 16 portadors como máximo).

• **Gestión de recursos radio**: establece, mantiene y libera las conexiones radio entre el móvil y la parte fija de la red. Petición de canal RACH. Control de potencia: garantizar que todos los móviles llegan con la misma potencia.

• **Gestión de movilidad**: localización de terminales, autentificación de usuarios y cifrado de las comunicaciones. La primera vez que un usuario accede a la red GSM, envía a su VLR (asociado a una MSC) el valor de LAI"Local Area Identification=0" e IMSI(En principio esta es la única vez que el IMSI viaja por el aire). El VLR crea entonces un espacio en la memoria con la direccion: LMSI, donde almacenar todos los datos del nuevo usuario.

El área de localización: conjunto de célculas dentro de la zona controalda por una VLR/MSC destinatarias de un mensaje de paging. Cada vez que un móvil cambia de área, éste lo detecta e inicia un proceso de actualización de la localización, para que la VLR y la HLR sea conocedoras de la nueva ubicación del móvil.

El VLR informa al HLR, cuya identificación está en el IMSI, del nuevo usuario que tiene localizado, le dal el IMSI y el LMSI y a cambio recibe los datos referentes al abonado: tripletas, servicios contratados, etc. En particular, a partir de las tripletas se puede proceder a autentificar al abonado en el MSC/VLR. Una vez identificado el abonado se le asigna un TMSI (Temporary Mobile Susbscriber Identity") que es un alias del IMSI y que es lo que viajará a partir de este momento por el aire en lugar del IMSI para evitar su intercepción. El TMSI reside entonces en el VLR (y se le asignará al móvil mientras no cambie de VLR) y en la SIM (no en el HLR).

Idle State: una vez se conmuta el terminal a ON(*Attach*) el móvil empieza a muestrear cada una de las señales RF recibidas y se queda con las 5 mejores: este proceso dura de 3 a 5 segundos. El móvil se queda con la señal de mayor nivel y mira si se trata de una portadora que transporte un BCCH, para ello debe detectar el Frequency Correction Burst.

En el caso de no ser una portadora adecuada, se pasa a la siguiente de la lista. Una vez se asegura de que la información de BCCH está disponible, el móvil acampa en la mencionada célula. El Móvil leerá el LAI transmitido en el canal BCCH (MCC Mobile Country Code 3, MNC mobile Network Code 2, LAC location Area Coder 16). Si el LAI es el mismo que el que tiene residente en la SIM correspondiente a la íltima LAI donde ha estado transitando, entra en el IDLE STATE", en caso contrario se procede a una actualización de la localización "location updating".

Location Updating: el BCCH informa de el LAI Location Area Identity de la base correspondiente, si el móvil se encuentra en un área distinta a la que el BCCH dice, se procede a una location update. E el mensaje de petición del móvil están la TMSI (Si se ha cambiado de VLR) y la LAI viejos, a partir de los cuales la red sabe cual es la VLR/MSC vieja donde dirigirse para recavar el IMSI y la tripleta de autentificación.

El VLR nuevo pide al móvil su IMSI en el caso que no reconozca el TMSI, con el que puede pedir información directamente al HLR. La VLR informa al HLR del móvil de se nueva posición: LAC, VLR. El *Detach* sirve para economizar la señalización del sistema.

Centro de autentificación: genera tres parámetros o tripletas (SRES, RAND y Kc) que se utilizane en los procesos de autentificación y cifrado.

Garantiza que el usuario móvil pertenece a la red gestionada por un determinado operador. La BTS envía el RAND y la red comprueba la identidad del usuario mediante la SRES recibida del móvil. Ki clave secreta de usuario, alamacenada en la SIM y en el centro de autentificación. En la parte de la red, los parámetros RAND y SRES son generados en el AUC y transferidos al HLR y VLR.

Autentificación: MS: RAND (128 bits) codificado con Ki(64 bits) algoritmo A3 = SRES.
Cifrado: añade privacidad al sistema, afecta tanto a los canales de tráfico como de control dedicado.

MS: A5(número de trama 22 bits, $A8_{64}(Ki_{64}, RAND_{128})$

- **Gestión de la comunicación**: control "end to end" de las llamadas (establecimiento, mantenimiento y liberación) y gestión de servicios sumplementarios.