UNIT II: Telecommunication system

GSM

GSM is the most successful digital mobile telecommunication system in the world today. It is used by over 800 million people in more than 190 countries. In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies. To avoid this situation for a second generation fully digital system, the group special mobile (GSM) was founded in 1982. This system was soon named the global system for mobile communications (GSM), with the specification process lying in the hands of ETSI (ETSI, 2002), (GSM Association, 2002).

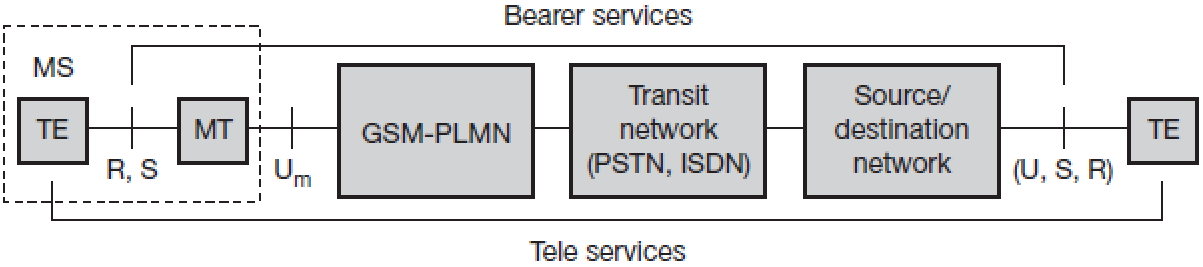
GSM Mobile services

GSM permits the integration of different voice and data services and the interworking with existing networks. Services make a network interesting for customers.

GSM has defined three different categories of services:

- Bearer services
- Tele services
- Supplementary services.

Figure shows a reference model for GSM services.



Bearer and Tele services reference model

A mobile station MS is connected to the GSM public land mobile network (PLMN) via the Um interface. (GSM-PLMN is the infrastructure needed for the GSM network.) This network is connected to transit networks, e.g., integrated services digital network (ISDN) or traditional public switched telephone network (PSTN). There might be an additional network, the source/destination network, before another terminal TE is connected. Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network, i.e., S in case of the mobile station, and a similar interface for the other terminal (e.g., S0 for ISDN terminals). Interfaces like U, S, and R in case of ISDN have not been defined for all networks, so it depends on the specific network which interface is used as a reference for the transparent transmission of data. In the classical GSM model, bearer services are connection-oriented and circuit- or packet-switched. These services only need the lower three layers of the ISO/OSI reference model.

Within the mobile station MS, the mobile termination (MT) performs all network specific tasks (TDMA, FDMA, coding etc.) and offers an interface for data transmission (S) to the terminal TE which can then be network independent. Depending on the capabilities of TE, further interfaces may be needed, such as R, according to the ISDN reference model (Halsall, 1996). Tele services are application specific and may thus need all seven layers of the ISO/OSI reference model. These services are specified end-to-end, i.e., from one terminal TE to another.

Bearer services

GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services. Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission. **Transparent bearer services** only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. The only mechanism to increase transmission quality is the use of **forward error correction (FEC)**, which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors.

Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a **radio link protocol (RLP)**. This protocol comprises mechanisms of **high-level data link control (HDLC)**, (Halsall, 1996) and special selective-reject mechanisms to trigger retransmission of erroneous data.

Tele services

GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g., fax).

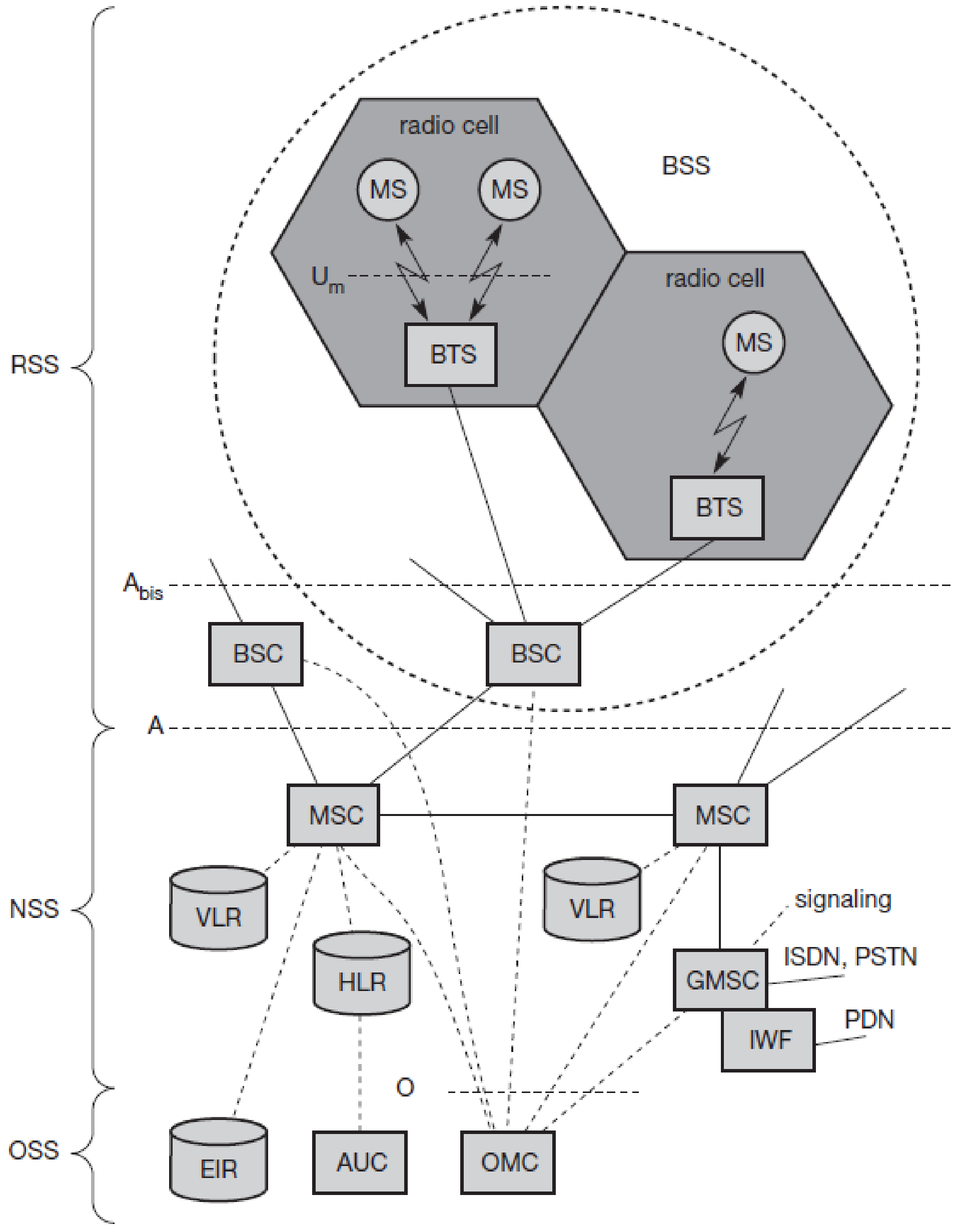
Another service offered by GSM is the **emergency number**. The same number can be used throughout country. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center.

A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters.

Supplementary services

In addition to tele and bearer services, GSM providers can offer **supplementary services**. Similar to ISDN networks, these services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user **identification**, call **redirection**, or **forwarding** of ongoing calls. Standard ISDN features such as **closed user groups** and **multiparty** communication may be available. Closed user groups are of special interest to companies because they allow, for example, a company-specific GSM sub-network, to which only members of the group have access

GSM ARCHITECTURE



A GSM system consists of three subsystems

- Radio sub system (RSS),
- Network and switching subsystem (NSS)
- Operation subsystem (OSS).

Radio subsystem

As the name implies, the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). Figure 4.4 shows the connection between the RSS and the NSS via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines).

- **Base station subsystem (BSS)**: A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- **Base transceiver station (BTS)**: A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to MS via the **Um interface** (ISDN U interface for mobile use), and to the BSC via the **Abis interface**. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) and will be discussed in more detail below. The Abis interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- **Base station controller (BSC)**: The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS)**: The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM.3 While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a **personal identity number (PIN)**, a **PIN unblocking key (PUK)**, an **authentication key Ki**, and the **international mobile subscriber identity (IMSI)** (ETSI, 1991c). The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM.

Network and switching subsystem

The "heart" of the GSM system is formed by the **network and switching subsystem (NSS)**. The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:

- **Mobile services switching center (MSC)**: MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as **PSTN** and **ISDN**. Using additional **interworking functions (IWF)**, an MSC can also connect to **public data networks (PDN)** such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

- **Home location register (HLR)**: The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**. Dynamic information is also needed, e.g., the current **location area (LA)** of the MS, the **mobile subscriber roaming number (MSRN)**, the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting.
- **Visitor location register (VLR)**: The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information.

Operation subsystem

The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance.

- **Operation and maintenance center (OMC)**: The OMC monitors and controls all other network entities via the O interface. Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
- **Authentication centre (AuC)**: As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
- **Equipment identity register (EIR)**: The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft.

Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible

Protocols

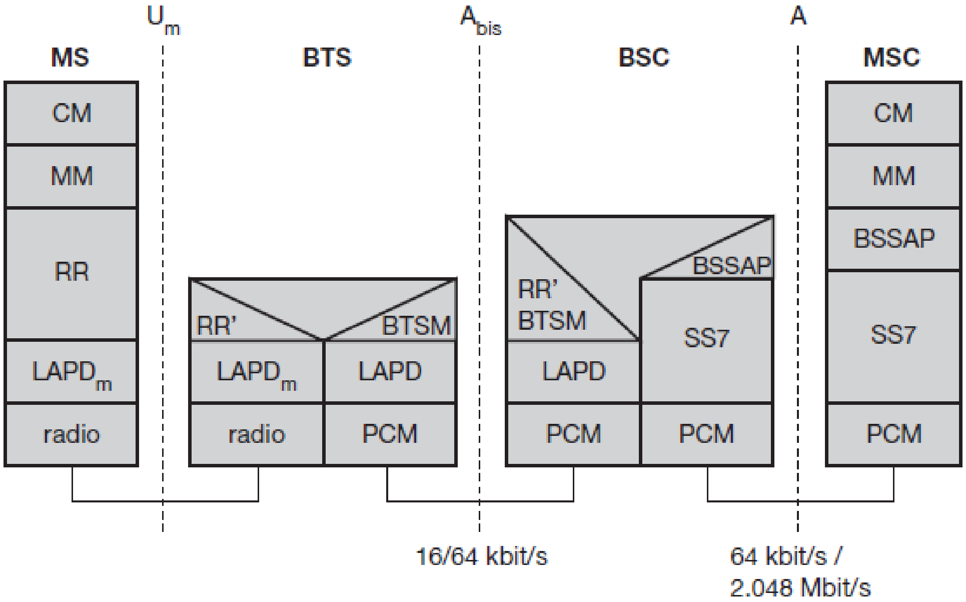


Figure shows the protocol architecture of GSM with signaling protocols, interfaces, as well as the entities. The main interest lies in the U_m interface, as the other interfaces occur between entities in a fixed network.

Layer 1, the physical layer, handles all radio-specific functions. This includes the creation of bursts according to the five different formats, multiplexing of bursts into a TDMA frame, synchronization with the BTS, detection of idle channels, and measurement of the channel quality on the downlink. The physical layer at Um uses GMSK for digital modulation and performs encryption/decryption of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface. The main tasks of the physical layer comprise channel coding and error detection/correction.

Signaling between entities in a GSM network requires higher layers. For this purpose, the $LAPD_m$ protocol has been defined at the U_m interface for layer two. $LAPD_m$, as the name already implies, has been derived from link access procedure for the D-channel (LAPD) in ISDN systems,. $LAPD_m$ is a lightweight LAPD because it does not need synchronization flags or check summing for error detection. $LAPD_m$ offers reliable data transfer over connections, re-sequencing of data frames, and flow control. As there is no buffering between layer one and two, $LAPD_m$ has to obey the frame structures, recurrence patterns etc., defined for the Um interface. Further services provided by $LAPD_m$ include segmentation and reassembly of data and acknowledged/unacknowledged data transfer.

The network layer in GSM, **layer three**, comprises several sub layers. The lowest sub layer is the **radio resource management (RR)**.Only a part of this layer, **RR**', is implemented in the BTS, the remainder is situated in the BSC. The functions of RR' are supported by the BSC via the **BTS management (BTSM)**. The main tasks of RR are setup, maintenance, and release of radio channels. RR also directly accesses the physical layer for radio information and offers a reliable connection to the next higher layer.

Mobility management (MM) contains functions for registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI) that replaces the international mobile subscriber identity (IMSI) and which hides the real identity of an MS user over the air interface. While the IMSI identifies a user, the TMSI is valid only in the current location area of a VLR. MM offers a reliable connection to the next higher layer.

Finally, the call management (CM) layer contains three entities: call control (CC), short message service (SMS), and supplementary service (SS). CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters.

Additional protocols are used at the A_{bis} and A interfaces. Data transmission at the physical layer typically uses pulse code modulation (PCM) systems.

Signaling system No. 7 (SS7) is used for signaling between an MSC and a BSC. This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. An MSC can also control a BSS via a **BSS application part (BSSAP)**.

DECT

Another fully digital cellular network is the digital enhanced cordless telecommunications (DECT) system specified by ETSI (2002, 1998j, k), (DECT Forum, 2002). Formerly also called digital European cordless telephone and digital European cordless telecommunications, DECT replaces older analog cordless phone systemssuch as CT1 and CT1+. These analog systems only ensured security to a limited extent as they did not use encryption for data transmission and only offered a relatively low capacity. DECT is also a more powerful alternative to the digital system CT2, which is mainly used in the UK (the DECT standard works throughout Europe), and has even been selected as one of the 3G candidates in the IMT-2000 family. DECT is mainly used in offices, on campus, at trade shows, or in the home. Furthermore, access points to the PSTN can be established within, e.g., railway stations, large government buildings and hospitals, offering a much cheaper telephone service compared to a GSM system. DECT could also be used to bridge the last few hundred meters between a new network operator and customers. Using this 'small range' local loop, new companies can offer their service without having their own lines installed in the streets. DECT systems offer many different interworking units, e.g., with GSM, ISDN, or data networks. Currently, over 100 million DECT units are in use (DECT, 2002). A big difference between DECT and GSM exists in terms of cell diameter and cell capacity. While GSM is designed for outdoor use with a cell diameter of up to 70 km, the range of DECT is limited to about 300 m from the base station (only around 50 m are feasible inside buildings depending on the walls). Due to this limited range and additional multiplexing techniques, DECT can offer its service to some 10,000 people within one km2. This is a typical scenario within a big city, where thousands of offices are located in skyscrapers close together. DECT also uses base stations, but these base stations together with a mobile station are in a price range of €100 compared to several €10,000 for a GSM base station. GSM base stations can typically not be used by individuals for private networks. One reason is licensing as all GSM frequencies have been licensed to network operators. DECT can also handle handover, but it was not designed to work at a higher speed (e.g., up to 250 km/h like GSM systems). Devices handling GSM and DECT exist but have never been a commercial success. DECT works at a frequency range of 1880–1990 MHz offering 120 full duplex channels. Time division duplex (TDD) is applied using 10 ms frames. The frequency range is subdivided into 10 carrier frequencies using FDMA, each frame being divided into 24 slots using TDMA. For the TDD mechanism 12 slots are used as uplink, 12 slots as downlink (see Figure 3.4). The digital modulation scheme is GMSK – each station has an average transmission power of only 10 mW with a maximum of 250 mW.

System architecture

A DECT system, may have various different physical implementation depending on its actual use. Different DECT entities can be integrated into one physical unit; entities can be distributed, replicated etc. However, all implementations are based on the same logical reference model of the system architecture A **global network** connects the local communication structure to the outside world and offers its services via the interface D1. Global networks could be integrated services digital networks (ISDN), public switched telephone networks (PSTN), public land mobile networks (PLMN), e.g., GSM, or packet switched public data network (PSPDN). The services offered by these networks include transportation of data and the translation of addresses and routing of data between the local networks.

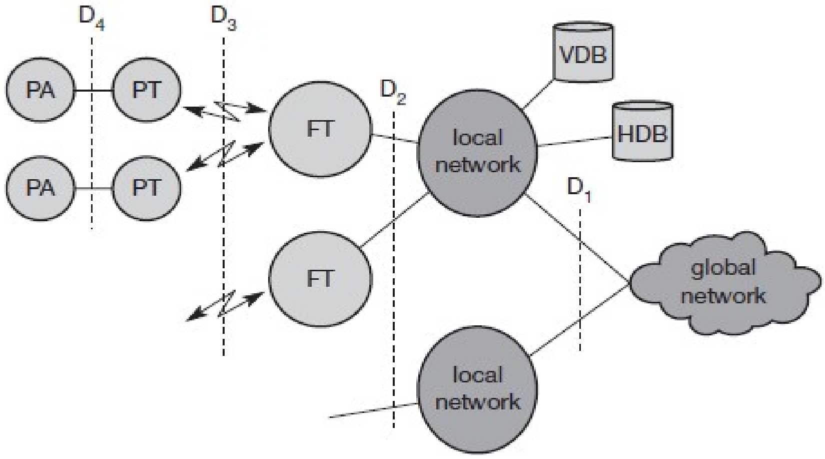


Figure 4.18
DECT system architecture reference model

Local networks in the DECT context offer local telecommunication services that can include everything from simple switching to intelligent call forwarding, address translation etc. Examples for such networks are analog or digital private branch exchanges (PBXs) or LANs, e.g., those following the IEEE 802.x family of LANs.

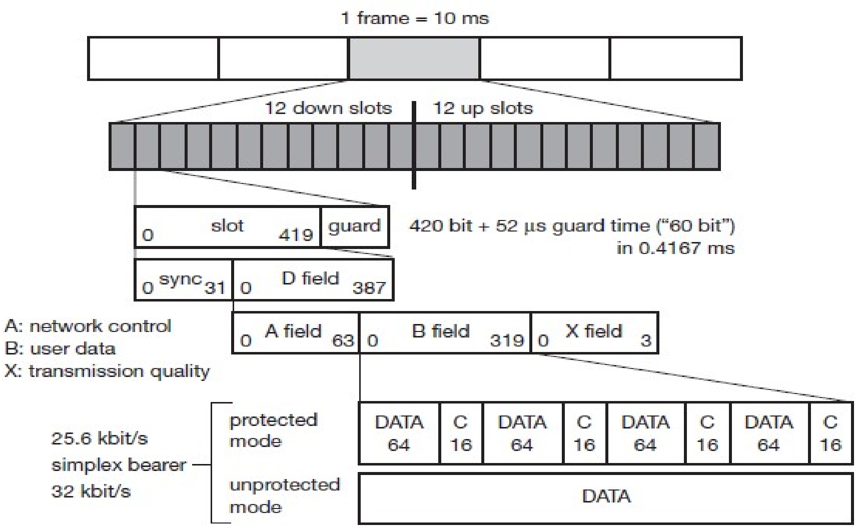


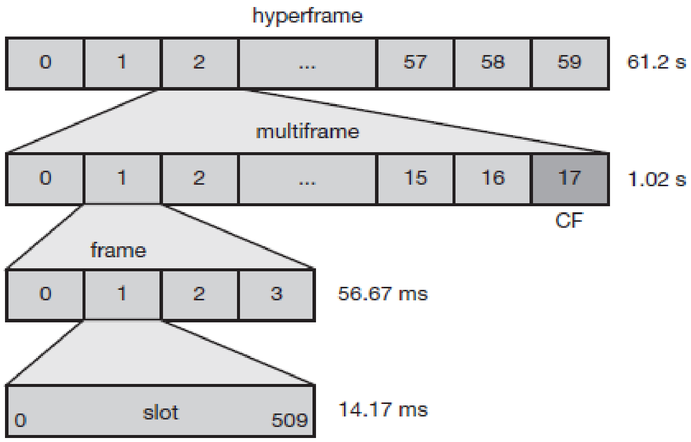
Figure 4.20
DECT multiplex and frame structure

As the core of the DECT system itself is quite simple, all typical network functions have to be integrated in the local or global network, where the databases **home data base (HDB)** and **visitor data base (VDB)** are also located. Both databases support mobility with functions that are similar to those in the HLR and VLR in GSM systems. Incoming calls are automatically forwarded to the current subsystem responsible for the DECT user, and the current VDB informs the HDB about changes in location. The DECT core network consists of the **fixed radio termination (FT)** and the **portable radio termination (PT)**, and basically only provides a multiplexing service. FT and PT cover layers one to three at the fixed network side and
mobile network side respectively. Additionally, several portable applications (PA) can be implemented on a device.

TETRA

Trunked radio systems constitute another method of wireless data transmission. These systems use many different radio carriers but only assign a specific carrier to a certain user for a short period of time according to demand. While, for example, taxi services, transport companies with fleet management systems and rescue teams all have their own unique carrier frequency in traditional systems, they can share a whole group of frequencies in trunked radio systems for better frequencyreuse via FDM and TDM techniques. These types of radio systems typically offer interfaces to the fixed telephone network, i.e., voice and data services, but are not publicly accessible. These systems are not only simpler than most other networks, they are also reliable and relatively cheap to set up and operate, as they only have to cover the region where the local users

Figure 4.21
TETRA frame structure



operate, e.g., a city taxi service. To allow a common system throughout Europe, ETSI standardized the **TETRA** system (**terrestrial trunked radio**)9 in 1991 (ETSI, 2002), (TETRA MoU, 2002). This system should replace national systems, such as MODACOM, MOBITEX and COGNITO in Europe that typically connect to an X.25 packet network. (An example system from the US is ARDIS.) TETRA offers two standards: the **Voice+Data (V+D)** service (ETSI, 1998l) and the **packet data optimized (PDO)** service (ETSI, 1998m). While V+D offers circuit-switched voice and data transmission, PDO only offers packet data transmission, either connection-oriented to connect to X.25 or connectionless for the ISO CLNS (connectionless network service). The latter service can be point-to-point or point-to-multipoint, the typical delay for a short message (128 byte) being less than 100 ms. V+D connection modes comprise unicast and broadcast connections, group communication within a certain protected group, and a direct ad hoc mode without a base station. However, delays for short messages can be up to 500 ms or higher depending on the priority. TETRA also offers bearer services of up to 28.8 kbit/s for unprotected data transmission and 9.6 kbit/s for protected transmission. Examples for end-to-end services are call forwarding, call barring, identification, call hold, call priorities, emergency calls and group joins. The system architecture of TETRA is very similar to GSM. Via the radio interface Um, the **mobile station (MS)** connects to the **switching and management infrastructure (SwMI)**, which contains the user data bases (HDB, VDB), the base station, and interfaces to PSTN, ISDN, or PDN. The system itself, however, is much simpler in real implementation compared to GSM, as typically no handover is needed. Taxis usually remain within a certain area which can be covered by one TETRA cell. Several frequencies have been specified for TETRA which uses FDD (e.g., 380–390 MHz uplink/390–400 MHz downlink, 410–420 MHz uplink/420–430 MHz downlink). Each channel has a bandwidth of 25 kHz and can carry

36 kbit/s. Modulation is DQPSK. While V+D uses up to four TDMA voice or data channels per carrier, PDO performs statistical multiplexing. For accessing a channel, slotted Aloha is used. typical **TDMA frame structure** of TETRA. Each **frame** consists of four slots (four channels in the V+D service per carrier), with a frame duration of 56.67 ms. Each **slot** carries 510 bits within 14.17 ms, i.e., 36 kbit/s. 16 frames together with one **control frame** (CF) form a **multiframe**, and finally,

a **hyperframe** contains 60 multiframes. To avoid sending and receiving at the same time, TETRA shifts the uplink for a period of two slots compared to the downlink. TETRA offers **traffic channels (TCH)** and **control channels (CCH)** similar to GSM. Typical TCHs are TCH/S for voice transmission, and TCH/7.2, TCH/4.8, TCH/2.4 for data transmission (depending on the FEC mechanisms required). However, in contrast to GSM, TETRA offers additional services like group call, acknowledged group call, broadcast call, and discreet listening. Emergency services need a sub-second group-call setup in harsh environments which possibly lack all infrastructure. These features are currently not available in GSM or other typical mobile telephone networks, so TETRA is complementary to other systems. TETRA has been chosen by many government organizations in Europe and China.

Localization and calling

One fundamental feature of the GSM system is the automatic, worldwide localization of users. The system always knows where a user currently is, and the same phone number is valid worldwide. To provide this service, GSM performs periodic location updates even if a user does not use the mobile station (provided that the MS is still logged into the GSM network and is not completely switched off).

The HLR always contains information about the current location (only the location area, not the precise geographical location), and the VLR currently responsible for the MS informs the HLR about location changes. As soon as an MS moves into the range of a new VLR (a new location area), the HLR sends all user data needed to the new VLR. **Changing VLRs with uninterrupted availability of all services is also called roaming**. Roaming can take place within the network of one provider, between two providers in one country (national roaming is, often not supported due to competition between operators), but also between different providers in different countries (international roaming).

To locate an MS and to address the MS, several numbers are needed:

- **Mobile station international ISDN number (MSISDN):** The only important number for a user of GSM is the phone number. The phone number is not associated with a certain device but with the SIM, which is personalized for a user. This number consists of the **country code (CC)** (e.g., +49 179 1234567 with 49 for Germany), the **national destination code (NDC)** (i.e., the address of the network provider, e.g., 179), and the **subscriber number (SN)**.
- **International mobile subscriber identity (IMSI):** GSM uses the IMSI for internal unique identification of a subscriber. IMSI consists of a mobile country code (MCC) (e.g., 240 for Sweden, 208 for France), the mobile network code (MNC) (i.e., the code of the network provider), and finally the mobile subscriber identification number (MSIN).
- **Temporary mobile subscriber identity (TMSI):** To hide the IMSI, which would give away the exact identity of the user signaling over the air interface, GSM uses the 4 byte TMSI for local subscriber identification. TMSI is selected by the current

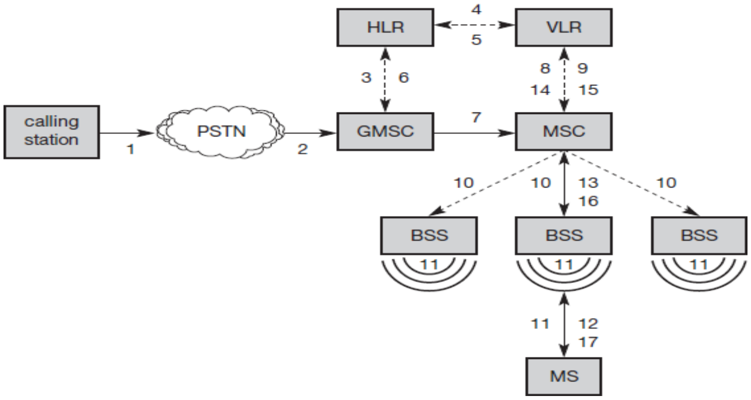
VLR and is only valid temporarily and within the location area of the VLR. Additionally, a VLR may change the TMSI periodically.

- **Mobile station roaming number (MSRN):** Another temporary address that hides the identity and location of a subscriber is MSRN. The VLR generates this address on request from the MSC, and the address is also stored in the HLR. MSRN contains the current **visitor country code (VCC)**, the **visitor national destination code (VNDC)**, the identification of the current MSC together with the subscriber number. The MSRN helps the HLR to find a subscriber for an incoming call.

Calling in GSM I of two types:

- Mobile terminated call (MTC)
- Mobile originated call (MOC)

Mobile terminated call (MTC)

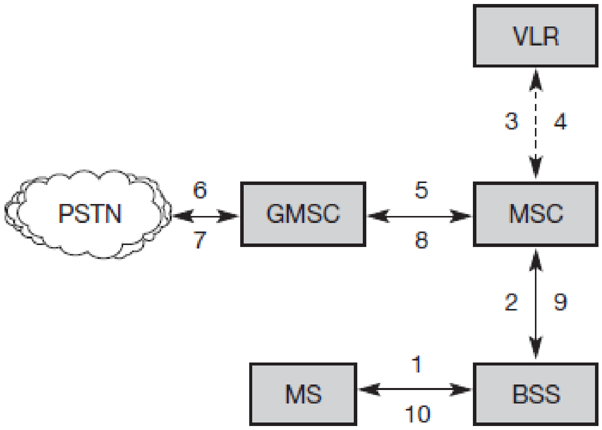


A situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station). Figure shows the basic steps needed to connect the calling station with the mobile user.

In step 1, a user dials the phone number of a GSM subscriber. The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC (2). The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR (3). The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR (4). After receiving the MSRN (5), the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC (6). The GMSC can now forward the call setup request to the MSC indicated (7).

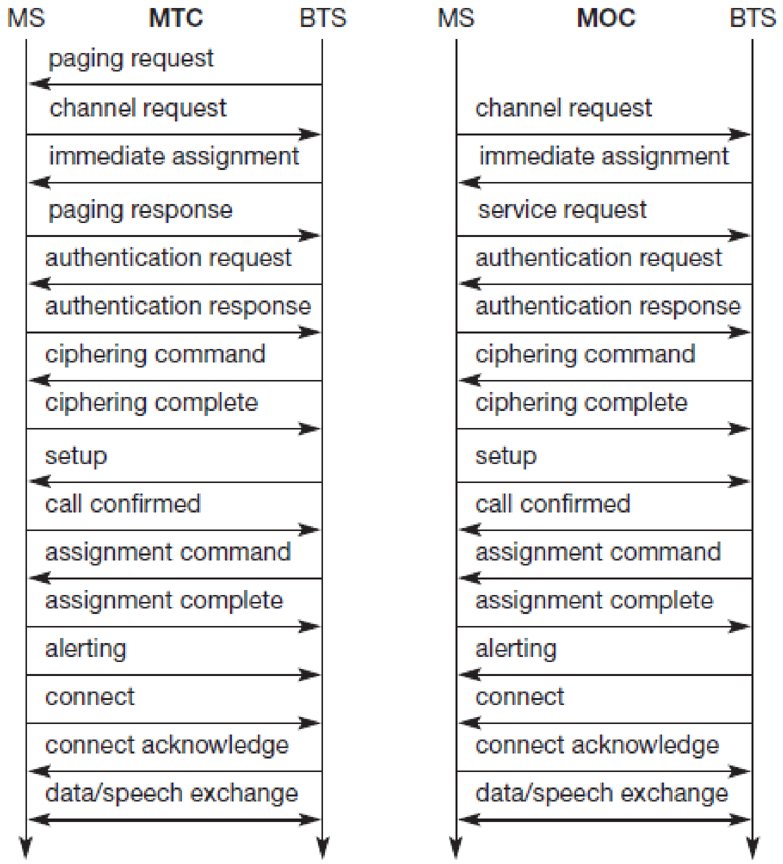
From this point on, the MSC is responsible for all further steps. First, it requests the current status of the MS from the VLR (8). If the MS is available, the MSC initiates paging in all cells it is responsible for (10), as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist). The BTSs of all BSSs transmit this paging signal to the MS (11). If the MS answers (12 and 13), the VLR has to perform security checks (set up encryption etc.). The VLR then signals to the MSC to set up a connection to the MS (steps 15 to 17).

Mobile originated call (MOC)



It is much simpler to perform a **mobile originated call (MOC)** compared to a MTC. The MS transmits a request for a new connection (1), the BSS forwards this request to the MSC (2). The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during onnection setup (in either direction).



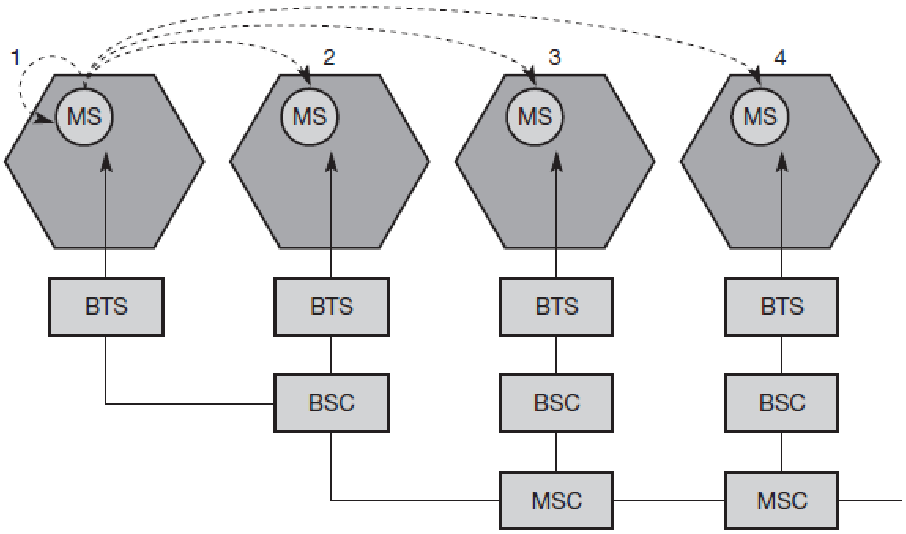
Message flow for MTC and MOC

Handover

Cellular systems require handover procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities. The smaller the cell size and the faster the movement of a mobile station through the cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required. However, a handover should not cause a cut-off, also called call drop. GSM aims at maximum handover duration of 60ms.

There are two basic reasons for a handover:

- The mobile station **moves out of the range** of a BTS or a certain antenna of a BTS respectively. The received **signal level** decreases continuously until it falls below the minimal requirements for communication. The **error rate** may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the **quality of the radio link** and make radio transmission impossible in the near future.
- The wired infrastructure (MSC, BSC) may decide that the **traffic in one cell is too high** and shift some MS to other cells with a lower load (if possible). Handover may be due to **load balancing**.



Types of handover in GSM

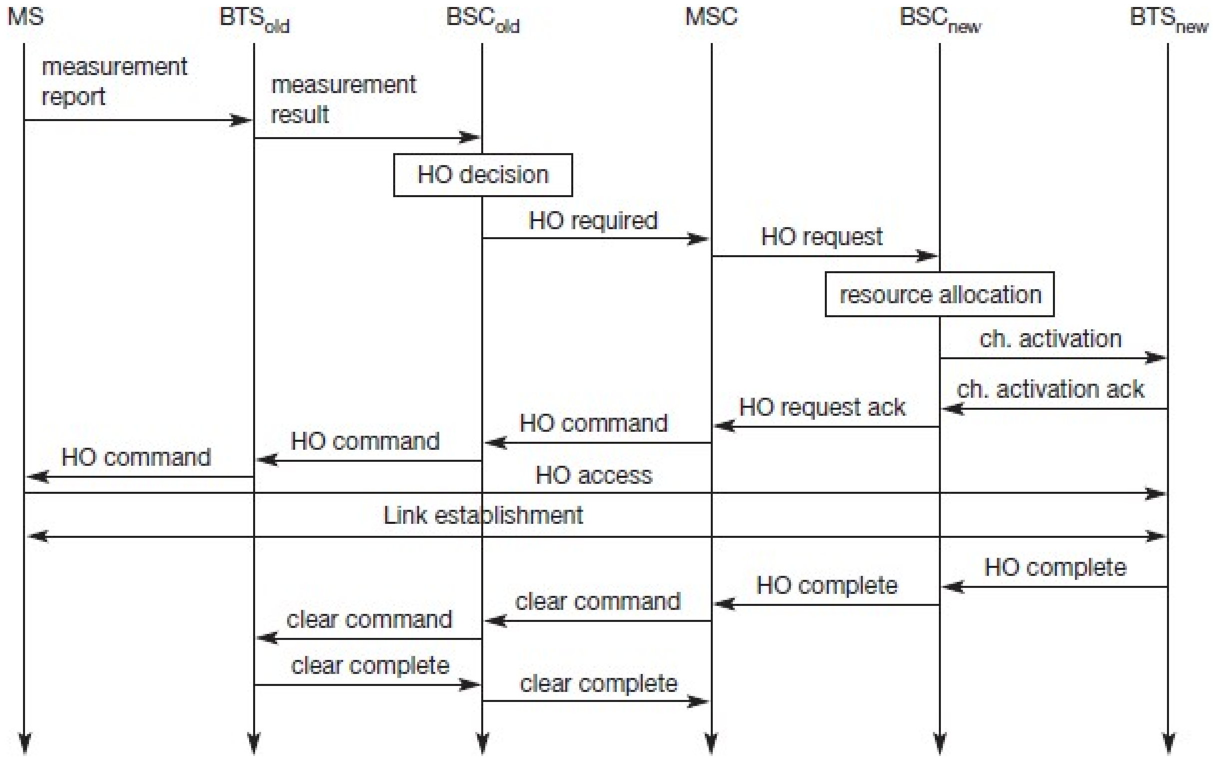
There are 4 scenarios of handover in GSM:

- **Intra-cell handover:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).
- **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).
- **Inter-BSC, intra-MSC handover:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).
- **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

For example following is the mechanism of the intra MSC handover:

Intra-MSC handover

To provide all the necessary information for a handover due to a weak link, MS and BTS both perform periodic measurements of the downlink and uplink quality respectively. Measurement reports are sent by the MS about every half-second and contain the quality of the current link used for transmission as well as the quality of certain channels in neighboring cells. The MS sends its periodic measurements reports, the BTS_{old} forwards these reports to the BSC_{old} together with its own measurements. Based on these values and, e.g., on current traffic conditions, the BSC_{old} may decide to perform a handover and sends the message $HO_{required}$ to the MSC. The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSC_{new}. This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTS_{new} to prepare for the arrival of the MS.



The BTS_{new} acknowledges the successful channel activation, BSC_{new} acknowledges the handover request. The MSC then issues a handover command that is forwarded to the MS. The MS now breaks its old radio link and accesses the new BTS. The next steps include the establishment of the link. Basically, the MS has then finished the handover, but it is important to release the resources at the old BSC and BTS and to signal the successful handover using the handover and clear complete messages as shown.

Security

GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS). The SIM stores personal, secret data and is protected with a PIN against unauthorized use. (For example, the secret key K_i used for authentication and encryption procedures is stored in the SIM.)

- **Access control and authentication:** The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication.
- **Confidentiality:** All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.

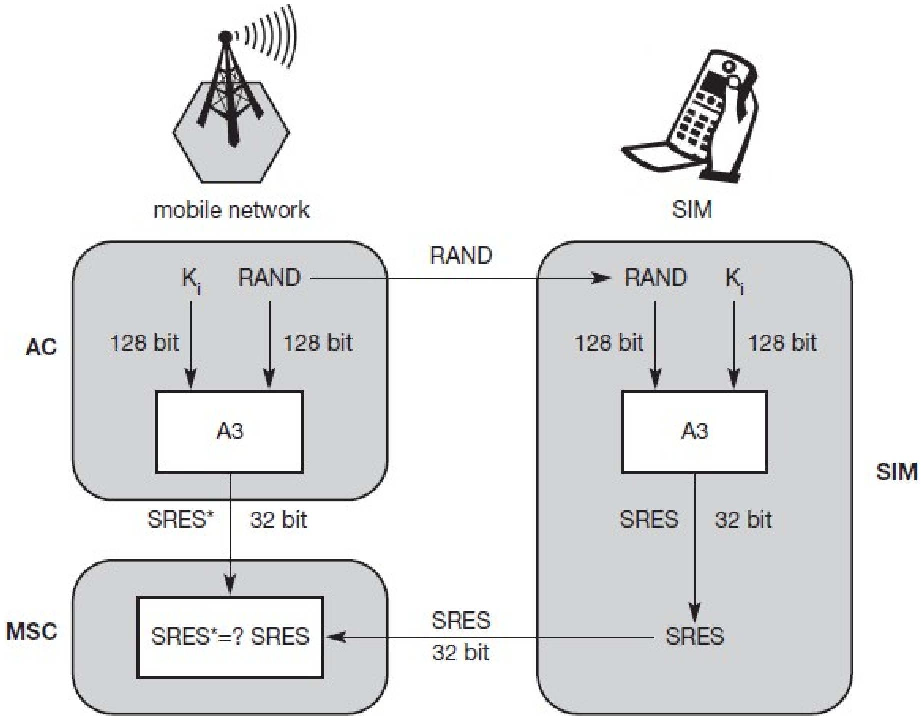
- **Anonymity:** To provide user anonymity, all data is encrypted before transmission, and user identifiers (which would reveal an identity) are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

Three algorithms have been specified to provide security services in GSM. Algorithm A3 is used for authentication, A5 for encryption, and A8 for the generation of a cipher key

Authentication

Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the individual authentication key K_i, the user identification IMSI, and the algorithm used for authentication A3. Authentication uses a challenge-response method: the access control AC generates a random number RAND as challenge, and the SIM within the MS answers with SRES (signed response) as response. The AuC performs the basic generation of random values RAND, signed responses SRES and cipher keys K_c for each IMSI, and then forwards this information to the HLR. The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR.

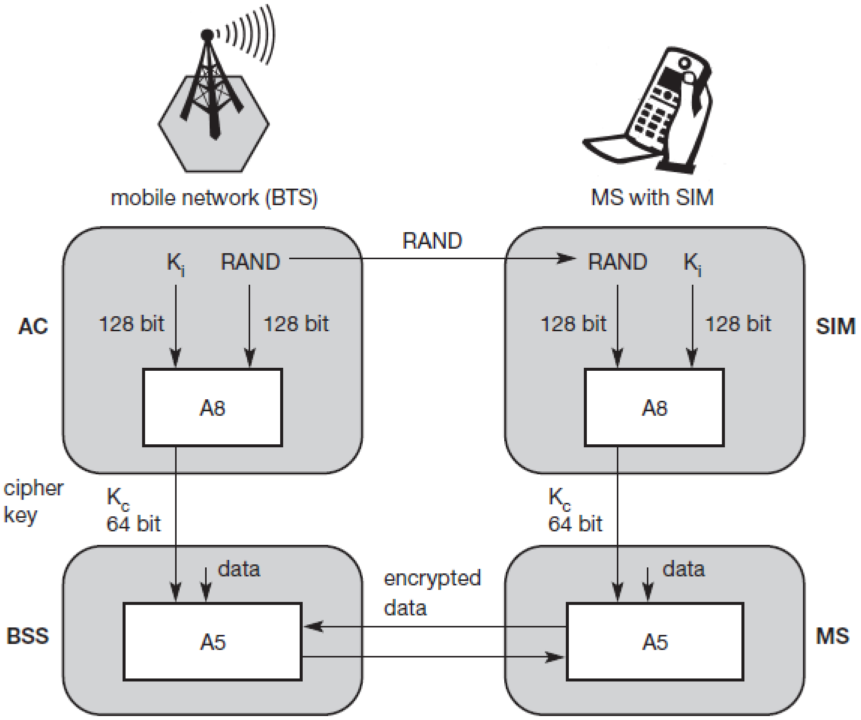
For authentication, the VLR sends the random value RAND to the SIM. Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called A3. The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.



Encryption

To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key Kc. Kc is generated using the individual key Ki and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same Kc based on the random value RAND. The key Kc itself is not transmitted over the air interface.

MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc. As Figure 4.15 shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping. However, the publication of A3 and A8 on the internet showed that in certain implementations 10 of the 64 bits are always set to 0, so that the real length of the key is thus only 54 consequently, the encryption is much weaker.



New data services

The standard bandwidth of 9.6 kbit/s available for data transmission is not sufficient for the requirements of today’s computers. When GSM was developed, not many people anticipated the tremendous growth of data communication compared to voice communication. At that time, 9.6 kbit/s was a lot, or at least enough for standard group 3 fax machines. But with the requirements of, e.g., web browsing, file download, or even intensive e-mail exchange with attachments, this is not enough.

To enhance the data transmission capabilities of GSM, two basic approaches are possible.

- HSCSD(High speed circuit switched data)
- GPRS(General packet radio service)

HSCSD

A straightforward improvement of GSM's data transmission capabilities is high speed circuit switched data (HSCSD), which is available with some providers. In this system, higher data rates are achieved by bundling several TCHs. An MS requests one or more TCHs from the GSM network, i.e., it allocates several TDMA slots within a TDMA frame. This allocation can be asymmetrical, i.e., more slots can be allocated on the downlink than on the uplink, which fits the typical user behavior of downloading more data compared to uploading. Basically, HSCSD only requires software upgrades in an MS and MSC.

In theory, an MS could use all eight slots within a TDMA frame to achieve an air interface user rate (AIUR) of, e.g., 8 TCH/F14.4 channels or 115.2 kbit/s. One problem of this configuration is that the MS is required to send and receive at the same time. Standard GSM does not require this capability – uplink and downlink slots are always shifted for three slots.

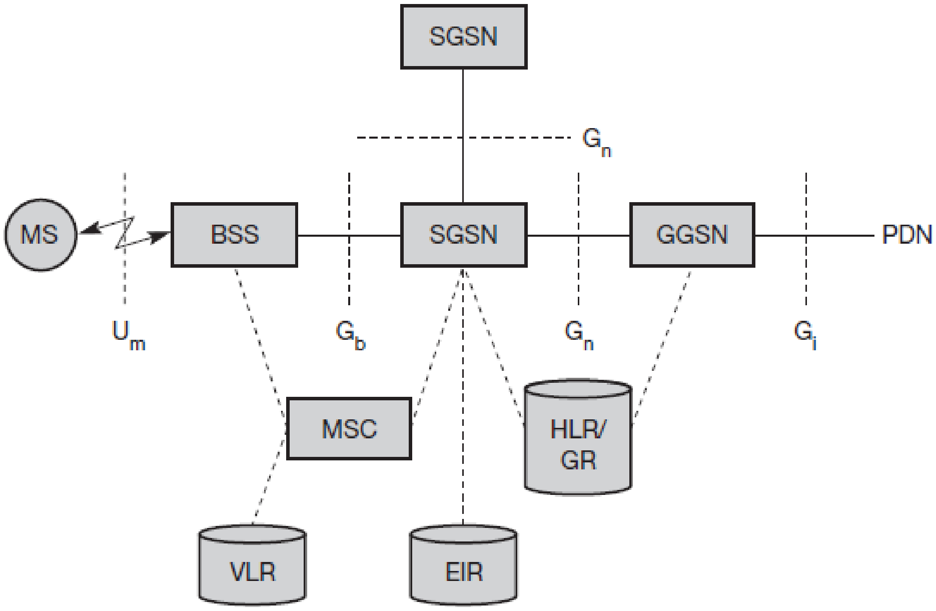
Although it appears attractive at first glance, HSCSD exhibits some major disadvantages. It still uses the connection-oriented mechanisms of GSM. These are not at all efficient for computer data traffic, which is typically bursty and asymmetrical. While downloading a larger file may require all channels reserved, typical web browsing would leave the channels idle most of the time. Allocating channels is reflected directly in the service costs, as once the channels have been reserved, other users cannot use them.

GPRS

The next step toward more flexible and powerful data transmission avoids the problems of HSCSD by being fully packet-oriented. The general packet radio service (GPRS) provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small volumes (e.g., typical web requests) or infrequent transmissions of small or medium volumes (e.g., typical web responses) according to the requirement specification.

The main concepts of GPRS are as follows. For the new GPRS radio channels, the GSM system can allocate between one and eight time slots within a TDMA frame. Time slots are not allocated in a fixed, pre-determined manner but on demand. All time slots can be shared by the active users; up- and downlink are allocated separately. Allocation of the slots is based on current load and operator preferences. Depending on the coding, a transfer rate of up to 170 kbit/s is possible. For GPRS, operators often reserve at least a time slot per cell to guarantee a minimum data rate.

GPRS architecture reference model



The **GPRS architecture** introduces two new network elements, which are called **GPRS support nodes (GSN)** and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined. The **gateway GPRS support node (GGSN)** is the interworking unit between the GPRS network and external **packet data networks (PDN)**. This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation. The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IP-based GPRS backbone network (Gn interface).

The other new element is the serving GPRS support node (SGSN) which supports the MS via the Gb interface. The SGSN, for example, requests user addresses from the GPRS register (GR), keeps track of the individual MSs' location, is responsible for collecting billing information (e.g., counting bytes), and performs several security functions such as access control. The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC. The GR, which is typically a part of the HLR, stores all GPRS-relevant data. GGSNs and SGSNs can be compared with home and foreign agents, respectively, in a mobile IP network.

Broadcast systems

. Typical broadcast systems, such as radio and television, distribute information regardless of the needs of individual users. As an addition to two-way communication technologies, broadcasting information can be very cost effective. Just imagine the distribution of a movie trailer to millions of potential customers and compare it with the abilities of 3G base stations to provide 10–20 simultaneous users with a 128 kbit/s video stream. The distribution of the trailer would block the whole mobile network for a long time even if tens of thousand base stations are assumed. In the future, television and radio transmissions will be fully digital. Already several radio stations produce and transmit their programmes digitally via the internet or digital radio (Digital television is on its way. Besides transmitting video and audio, digital transmission allows for the distribution of arbitrary digital data, i.e., multimedia information can accompany radio and TV programmes at very low cost compared to individual wireless connections.

Cyclical repetition of data

A broadcast sender of data does not know when a receiver starts to listen to the transmission. While for radio or television this is no problem (if you do not listen you will not get the message), transmission of other important information, such as traffic or weather conditions, has to be repeated to give receivers a chance to receive this information after having listened for a certain amount of time (like the news every full hour). The cyclical repetition of data blocks sent via broadcast is often called a broadcast disk according to the project in Acharya (1995) or data carousel, e.g., according to the DAB/DVB standards (ETSI, 2002).

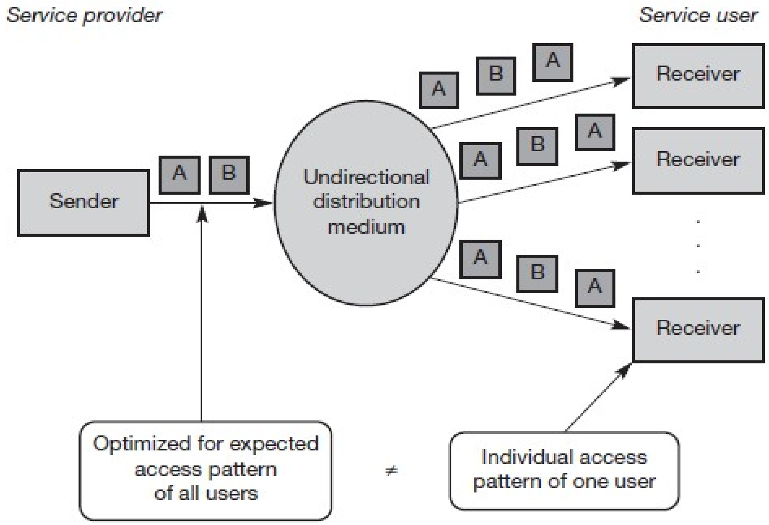

Service provider
Service user
Sender
A
B
Undirectional distribution medium
Receiver
Receiver
Receiver
A
B
A
Optimized for expected access pattern of all users
≠
Individual access pattern of one user

Figure 6.1
Broadcast transmission

Different patterns are possible (The sender repeats the three data blocks A, B, and C in a cycle. Using a flat disk, all blocks are repeated one after another. Every block is transmitted for an equal amount of time, the average waiting time for receiving a block is the same for A, B, and C.

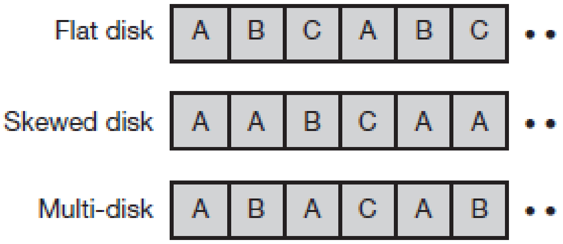


Figure 6.2
Different broadcast patterns

Skewed disks favor one or more data blocks by repeating them once or several times. This raises the probability of receiving a repeated block (here A) if the block was corrupted the first time. Finally, multi-disks distribute blocks that are repeated more often than others evenly over the cyclic pattern. This minimizes the delay if a user wants to access, e.g., block A.

Digital audio broadcasting

Today's analog radio system still follows the basic principle of frequency modulation invented back in 1933. In addition to audio transmission, very limited information such as the station identification can accompany the program. Transmission quality varies greatly depending on multi-path effects and interference. The fully digital DAB system does not only offer sound in a CD-like quality, it is also practically immune to interference and multi-path propagation effects (ETSI, 2001a), (DAB, 2002). DAB systems can use single frequency networks (SFN), i.e., all senders transmitting the same radio program operate at the same frequency. Today, different senders have to use different frequencies to avoid interference although they are transmitting the same radio program. Using an SFN is very frequency efficient, as a single radio station only needs one frequency throughout the whole country. Additionally, DAB transmission power per antenna is orders ofmagnitude lower compared to traditional FM stations. DAB uses VHF and UHF frequency bands (depending on national regulations), e.g., the terrestrial TV channels 5 to 12 (174–230 MHz) or the L-band (1452–1492 MHz). The modulation scheme used is DQPSK. DAB is one of the systems using COFDM (with 192 to 1536 carriers (the so-called ensemble) within a DAB channel of 1.5 MHz. Additionally, DAB uses FEC to reduce the error rate and introduces guard spaces between single symbols during transmission. COFDM and the use of guard spaces reduce ISI to a minimum. DAB can even benefit from multipath propagation by recombining the signals from different paths Within every frequency block of 1.5 MHz, DAB can transmit up to six stereo audio programmes with a data rate of 192 kbit/s each. Depending on the redundancy coding, a data service with rates up to 1.5 Mbit/s is available as an alternative. For the DAB transmission system, audio is just another type of data *(besides different coding schemes). DAB uses two basic transport mechanisms:*

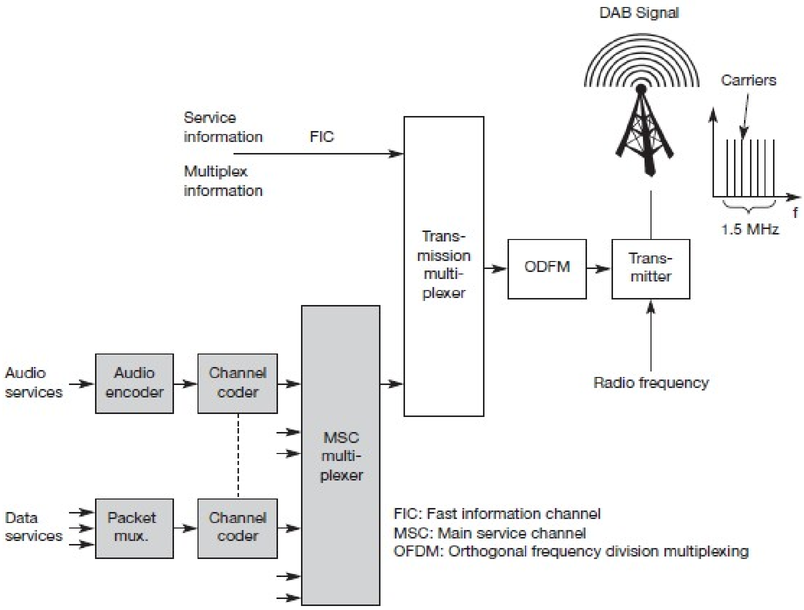


Figure 6.4
Components of a DAB sender (simplified)

● Main service channel (MSC): The MSC carries all user data, e.g. audio, multimedia data. The MSC consists of common interleaved frames (CIF), i.e., data fields of 55,296 bits that are sent every 24 ms (this interval depends on the transmission mode (ETSI, 2001a)). This results in a data rate of 2.304 Mbit/s. A CIF consists of capacity units (CU) with a size of 64 bits, which form the smallest addressable unit within a DAB system.

● Fast information channel (FIC): The FIC contains fast information blocks (FIB) with 256 bits each (16 bit checksum). An FIC carries all control information which is required for interpreting the configuration and content of the MSC. Two transport modes have been defined for the MSC. The stream mode offers a transparent data transmission from the source to the destination with a fixed bit rate in a sub channel. A sub channel is a part of the MSC and comprises several CUs within a CIF. The fixed data rate can be multiples of 8 kbit/s. The packet mode transfers data in addressable blocks (packets). These blocks are used to convey MSC data within a sub channel. DAB defines many service information structures accompanying an audio stream. This program associated data (PAD) can contain program information, control information, still pictures for display on a small LCD, title display etc. Audio coding uses PCM with a sampling rate of 48 kHz and MPEG audio compression. Each frame consists of three parts. The synchronization channel (SC) marks the start of a frame. It consists of a null symbol and a phase reference symbol to synchronize the receiver. The fast information channel (FIC) follows, containing control data in the FIBs. Finally, the main service channel (MSC) carries audio and data service components. . Audio services are encoded (MPEG compression) and coded for transmission (FEC). All data services are multiplexed and also coded with redundancy. The MSC multiplexer combines all user data streams and forwards them to the transmission multiplexer. This unit creates the frame structure by interleaving the FIC. Finally, OFDM coding is applied and the DAB signal is transmitted.

Digital video broadcasting

The logical consequence of applying digital technology to radio broadcasting is doing the same for the traditional television system. The analog system used today has basically remained unchanged for decades. The only invention worth mentioning was the introduction of color TV for the mass market back in the 1960s. Television still uses the low resolution of 625 lines for the European PAL system or only 525 lines for the US NTSC respectively2. The display is interlaced with 25 or 30 frames per second respectively. So, compared with today's computer displays with resolutions of 1,280 × 1,024 and more than 75 Hz frame rate, non-interlaced, TV performance is not very impressive. There have been many attempts to change this and to introduce digital TV with higher resolution, better sound and additional features, but no approach has yet been truly successful. One reason for this is the huge number of old systems that are installed and cannot be replaced as fast as computers (we can watch the latest movie on an old TV, but it is impossible to run new software on older computers!).

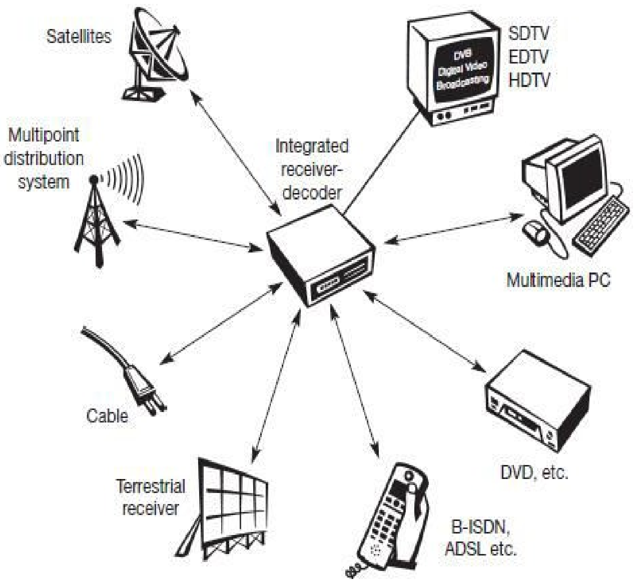


Figure 6.7
Digital video
broadcasting scenario

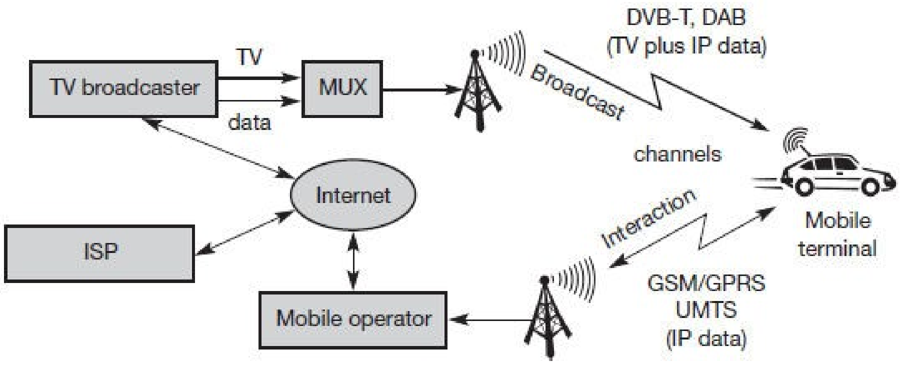
Varying political and economic interests are counterproductive to a common standard for digital TV. One approach toward such a standard, which may prove useful for mobile communication, too, is presented in the following sections. After some national failures in introducing digital TV, the so-called European Launching Group was founded in 1991 with the aim of developing a common digital television system for Europe. In 1993 these common efforts
were named digital video broadcasting (DVB) (Reimers, 1998), (DVB, 2002). Although the name shows a certain affinity to DAB, there are some fundamental differences regarding the transmission technology, frequencies, modulation etc.

The goal of DVB is to introduce digital television broadcasting using satellite transmission (DVB-S, (ETSI, 1997)), cable technology (DVB-C, (ETSI, 1998)), and also terrestrial transmission (DVB-T, (ETSI, 2001b)). components that should be integrated into the DVB architecture. The center point is an integrated receiver-decoder (set-top box) connected to a high-resolution monitor. This set-top box can receive DVB signals via satellites, terrestrial local/regional senders (multi-point distribution systems, terrestrial receiver), cable, B-ISDN, ADSL, or other possible future technologies. Cable, ADSL, and B-ISDN connections also offer a return channel, i.e., a user can send data such as channel selection, authentication information, or a shopping list. Audio/video streams can be recorded, processed, and replayed using digital versatile disk (DVD) or multimedia PCs. Different levels of quality are envisaged: standard definition TV (SDTV), enhanced definition TV (EDTV), and high definition TV (HDTV) with a resolution of up to 1,920 × 1,080 pixels. Similar to DAB, DVB also transmits data using flexible containers. These containers are basically MPEG-2 frames that do not restrict the type of information. DVB sends service information contained in its data stream, which specifies the content of a container.

Convergence of broadcasting and mobile communications

To enable the convergence of digital broadcasting systems and mobile communicationsystems ETSI (2000) and ETSI (1999d) define interaction channels through GSM for DAB andDVB, respectively. An interaction channel is not only common to DAB and DVB but covers alsodifferent fixed and mobile systems (UMTS, DECT, ISDN, PSTN etc.). 3G systems are typicallycharacterized by very small cells, especially in densely populated areas. Although 3G systems offerhigher data rates than 2G systems, their design has not fully taken into consideration the integrationof broadcast quality audio and TV services onto 3G terminals. This is true from a technical point ofview (capacity per cell in bit/s) as well as from an economic point of view (very high deploymentcost for full coverage, typically low return on invest for video services). High bandwidth audio andvideo is sent together with IP data via the broadcast channel. IP data could use multi-casting, datacarousels etc. as described above. For example, IP data in a DVB-T carousel could contain the top hundred web pages of the ISP's portal. Individual pages for single users are then additionally sent via GRPS or UMTS (DRiVE, 2002).

Figure 6.10
Mobile Internet services using IP over GSM/GPRS or UMTS as interaction channel for DAB or DVB


DVB-T, DAB
(TV plus IP data)
TV
TV broadcaster
MUX
data
Broadcast
channels
Internet
Interaction
Mobile
terminal
ISP
GSM/GPRS
UMTS
(IP data)
Mobile operator