Overview of GSM: The Global System for Mobile Communications

John Scourias
University of Waterloo
jscourias@neumann.uwaterloo.ca

March 13, 1996

1 History of GSM

During the early 1980s, analog cellular telephone systems experienced rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

- Good subjective speech quality
- Low terminal and service cost
- Support for international roaming

- Ability to support handhald terminals
- Support for range of new services and facilities
- Spectral efficiency
- ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and Phase 1 of the GSM specifications was published in 1990. Commercial service was started in mid-1991, and since then has experienced tremendous growth. Although standardized in Europe, GSM is not only a European standard. GSM networks are operational or planned in Europe, the Middle East, the Far East, Africa, North and South America, and Australia. By 1993 there were 36 GSM networks in 22 countries, with 25 additional countries having already selected or considering GSM [6]. In the beginning of 1994, there were 1.3 million subscribers worldwide [18]. By the beginning of 1995, there were over 5 million subscribers worldwide, and by September 1995 there were over 7.5 million subscribers in Europe alone [21]. With North America making a delayed entry into the GSM field, with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. Several thousand pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee the proper interworking between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

2 Services provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signalling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved.

Using the ITU-T definitions, telecommunication services can be divided into bearer services, teleservices, and supplementary services. The most basic teleservice supported by GSM is telephony. Speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911 in North America).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bidirectional service for short alphanumeric messages, up to 160 bytes. Messages are transported in a store-and-forward fashion. Point-to-point SMS involves the sending of a message to a Short Message Service Center (SM-SC), which is outside the scope of the GSM specifications. Receipt of the message by the SM-SC is acknowledged, and the SM-SC will forward the message to its destination, even if the receiving subscriber is temporarily unavailable. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates to all mobile stations in the cell that are subscribed to the service. Messages can be stored in the SIM card for later retrieval [2].

Supplementary services are provided on top of teleservices or bearer services. In the Phase 1

specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services are provided in the Phase 2 specifications, such as caller identification, call waiting, multi–party conversations.

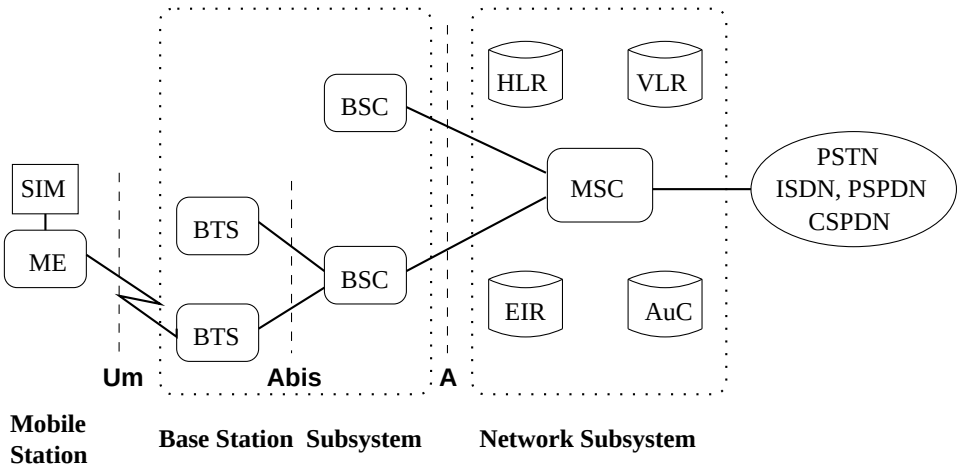
3 Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 1 shows the layout of a generic GSM network. The GSM network can be divided into three broad sections. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as handling mobility management. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.

3.1 Mobile Station

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, allowing the user to have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and



SIM Subscriber Identity Module BSC Base Station Controller MSC Mobile services Switching Center
ME Mobile Equipment HLR Home Location Register EIR Equipment Identity Register
BTS Base Transceiver Station VLR Visitor Location Register AuC Authentication Center

Figure 1: Architecture of a GSM network

the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

3.2 Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio tranceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile services Switching Center (MSC).

3.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a *mobile* subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjuction with several functional entities, which together with the MSC form the Network Subsystem. The MSC provides the connection to fixed networks, such as the PSTN or ISDN. Signalling between functional entities in the Network Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call routing and roaming capabilities of GSM. The HLR is a database that contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the SS7 signalling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signalling required. Note that the MSC contains no information about particular mobile stations — this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication of the subscriber, as well as encryption over the radio channel.

4 Radio link aspects

The International Telecommunication Union (ITU), which manages the international allocation of radio spectrum (among many other functions), allocated the bands 890-915 MHz for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station) for mobile networks in Europe. Since this range was already being used in the early 1980s by analog systems, the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed. Eventually, GSM will be allocated the entire 2x25 MHz bandwidth.

4.1 Multiple access and channel structure

Since radio spectrum is a limited resource shared by all users, a method must be devised to divide up the bandwidth among as many users as possible. The method chosen by GSM is a combination of Time- and Frequency-Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies of 200 kHz bandwidth. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme, The fundamental unit of time in this TDMA scheme is called a *burst period* and it lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a *TDMA frame* (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One logical channel is one burst period per TDMA

frame.

Channels are defined by the number and position of their corresponding burst periods. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used by mobile stations in *idle mode*.

4.1.1 Traffic channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is defined to be 120 ms (for compatibility with ISDN), which is how the length of a burst period is defined (120 ms $\div$ 26 frames $\div$ 8 burst periods per frame). TCHs are always allocated with a Slow Associated Control Channel (SACCH), which is used for signalling information related to the TCH, such as handover measurements. A TCH slot may be pre-empted for signalling information by setting the stealing flag associated with each information block on a time slot burst. This is called the Fast Associated Control Channel FACCH).

Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see Figure 2). TCHs for the uplink and downlink are by definition separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics. In addition to these *full-rate* TCHs, there are also *half-rate* TCHs defined, although they are not yet implemented. Half-rate TCHs will effectively double the capacity of a system. Eighth-rate TCHs are also specified, and are used for signalling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

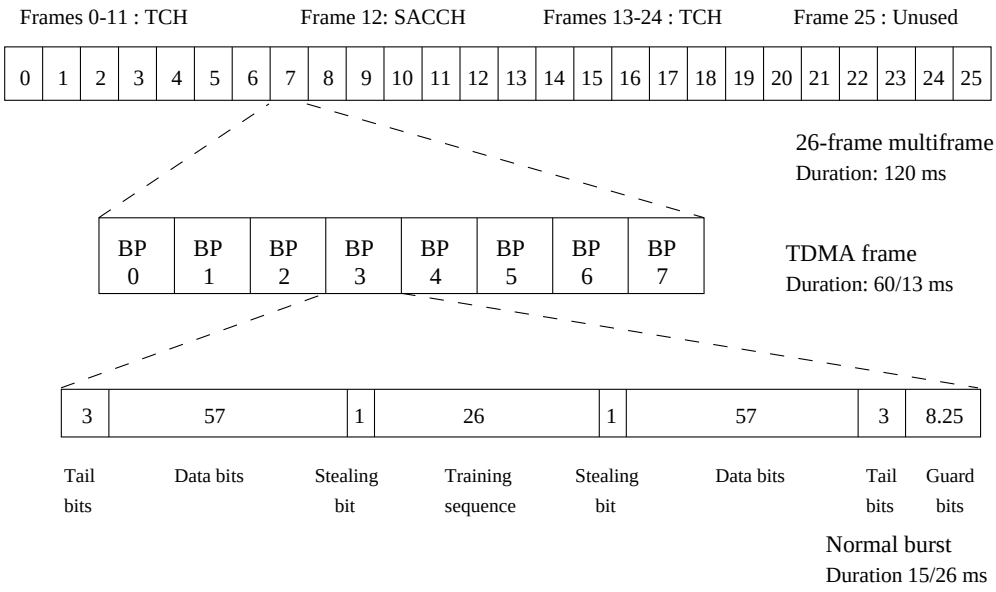


Figure 2: Organization of bursts, TDMA frames, and multiframes for speech and data

4.1.2 Control channels

Common channels can be accessed both by idle mode and dedicated mode mobile stations. The common channels are used by idle mode mobiles to exchange signalling information required to change to dedicated mode, to listen for paging messages for incoming calls, and to perform location management. Mobiles already in dedicated mode monitor the control channels surrounding base stations (specifically the Broadcast Control Channel) for handover and other information. The common channels are defined within a 51-frame multiframe, so that dedicated mobiles using the 26-frame multiframe TCH structure can still monitor control channels. The common channels include:

Broadcast Control Channel (BCCH) Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency hopping sequences.

Frequency Correction Channel (FCCH) *and* **Synchronisation Channel (SCH)** Used to synchronise the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).

Random Access Channel (RACH) Slotted Aloha channel used by the mobile to request a dedicated channel.

Paging Channel (PCH) Used to alert the mobile station of an incoming call.

Access Grant Channel (AGCH) Used to allocate an SDCCH to a mobile for signalling (in order to obtain a dedicated channel), following a request on the RACH.

4.1.3 Radio burst structure

There are four different types of radio bursts used for transmission in GSM [16]. The normal burst is used to carry data and most signalling. It has a total length of 156.25 bits, made up of two 57 bit information blocks, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 2. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.

The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts and provides information needed for synchronization. The access burst is shorter than the normal burst, and is used only on the RACH.

4.2 Speech coding

GSM uses digital transmission, so speech, which is inherently analog, has to be converted to a digital signal. The method employed by ISDN, and by current telephone systems for multiplexing

voice lines over high speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited – Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not change very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded using 260 bits, giving a total bit rate of 13 kbps.

4.3 Channel coding and modulation

Radio signals in a cellular environment are subject to many forms of degradation, including propagation losses, multipath fading, and co-channel interference. Encoded speech or data signals transmitted over the radio interface must therefore be protected as much as possible from such errors. Due to its digital nature, GSM is able to use error correction and detection codes, such as convolutional encoding and parity bits, and block interleaving to achieve this protection. The exact algorithms used differ for speech and for different data rates. The method used for speech blocks will be described below.

Recall that the speech codec produces a 260 bit block for every 20 ms speech sample. From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others. The bits are thus divided into three classes:

Class Ia 50 bits most sensitive to bit errors

Class Ib 132 bits moderately sensitive to bit errors

Class II 78 bits least sensitive to bit errors

Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection. If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded. It is replaced by a slightly attenuated version of the previous correctly received frame. These 53 bits, together with the 132 Class Ib bits and a 4 bit tail sequence (a total of 189 bits), are input into a 1/2 rate convolutional encoder of constraint length 4. Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolutional encoder thus outputs 378 bits, to which are added the 78 remaining Class II bits, which are unprotected. Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps.

To further protect against the burst errors common to the radio interface, each sample is interleaved. The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts. Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

As mentioned earlier, each time-slot burst is transmitted at a gross bit rate of 270.833 kbps. This digital signal is modulated onto the analog carrier frequency, which has a bandwidth of 200 kHz, using Gaussian-filtered Minimum Shift Keying (GMSK). GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions. The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station. The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled so as to limit adjacent channel interference, and for the time being, allow for the co-existence of GSM and the older analog systems.

4.4 Multipath equalization

At the 900 MHz range, radio waves bounce off everything — buildings, hills, cars, airplanes, etc. Multipath fading occurs when many reflected signals, each with a different phase, can reach the receiving antenna. Equalization is used to extract the desired signal from the unwanted reflections. It tries to determine how a known transmitted signal is modified by multipath fading, and constructs an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training

sequence transmitted in the middle of every time slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

4.5 Frequency hopping

The mobile station already has to be frequency agile, meaning it can move between a transmit, receive, and monitor time slot within one TDMA frame, which normally are on different frequencies. GSM makes use of this inherent frequency agility to implement slow frequency hopping, where the mobile and BTS transmit each TDMA frame on a different carrier frequency. The frequency hopping algorithm is specified by two parameters which are broadcast on the Broadcast Control Channel. Since multipath fading is dependent on carrier frequency, slow frequency hopping helps alleviate the problem. In addition, co-channel interference is in effect randomized. Another benefit is improved security and privacy.

4.6 Discontinuous transmission

Minimizing co-channel interference is a goal in any cellular system, since it allows better quality of service for a given cell size, or the use of smaller cells, thus increasing the overall capacity of the system. Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time in normal conversation [22], by turning the transmitter off during silence periods. An added benefit of DTX is that power is conserved at the mobile unit.

The most important component of DTX is, of course, Voice Activity Detection. It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise. If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called *clipping* is heard at the receiving end. If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased. Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to

the digital nature of GSM. To assure the receiver that the connection is not dead, *comfort noise* is created at the receiving end by trying to match the characteristics of the transmitting end's background noise.

4.7 Discontinuous reception

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its assigned sub-channel. The description of the sub-channel structure is transmitted on the BCCH. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

4.8 Power control

There are five classes of GSM mobile stations, defined according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Stations operate at the lowest power level that will maintain an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dB, from the peak power for the class down to a minimum of 13 dBm (20 milliwatts).

The mobile station measures the signal strength or signal quality (based on the bit error ratio), and sends the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability. This arises from having mobiles in co-channel cells alternatingly increase their power in response to increased co-channel interference caused by the other mobile increasing its power.

5 Network aspects

Ensuring the transmission of voice or data of a given quality over the radio link is only part of the function of a cellular mobile network. The fact that the geographical area covered by the network is divided into cells necessitates the implementation of a handover mechanism. Also, the fact that the mobile can roam nationally and internationally in GSM requires that registration, authentication, call routing and location updating functions exist in the GSM network. All these functions are handled through signalling protocols between different GSM entities.

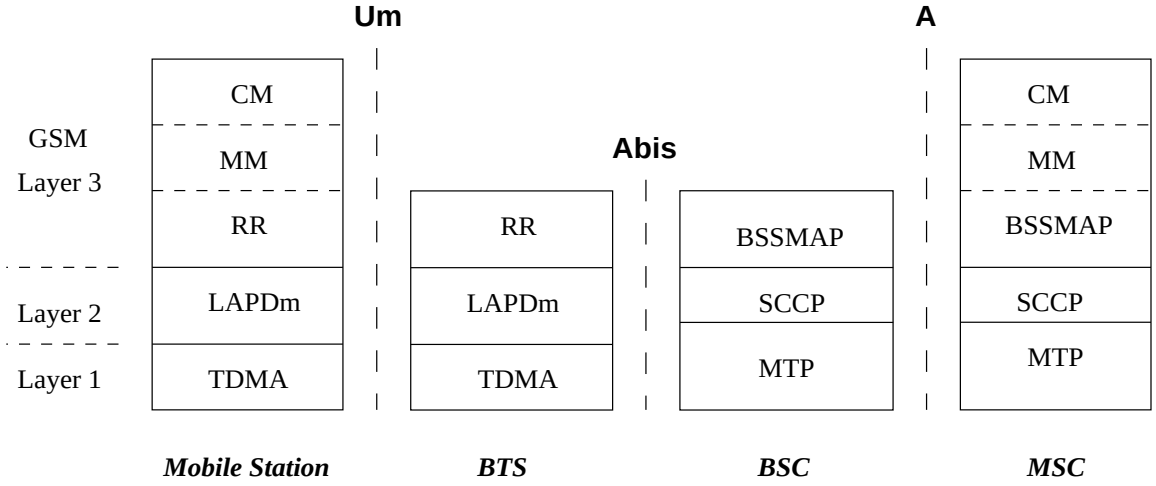


Figure 3: Signalling protocol structure in GSM

The signalling protocol in GSM is structured into three layers [19, 1], as shown in Figure 3. Layer 1 is the physical layer, which uses the channel structures discussed above over the radio link. Layer 2 is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of Signalling System Number 7 is used. Layer 3 of the GSM signalling protocol is itself divided into 3 sublayers.

Radio Resources Management Controls the setup, maintenance, and termination of radio and

fixed channels, including handovers.

Mobility Management Manages the location updating and registration procedures, as well as security and authentication.

Connection Management Handles general call control, similar to CCITT Recommendation Q.931, and manages Supplementary Services and the Short Message Service.

Signalling between the different entities in the fixed part of the network, such as between the HLR and VLR, uses the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signalling System Number 7). The specification of the MAP is quite complex, and at over 800 pages, it is one of the longest documents in the GSM recommendations.

5.1 Radio resources management

The Radio Resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the mobile station, and the Base Station Subsystem, as well as the MSC. The RR layer is concerned with the management of an RR-session [16], which is the total time that a mobile is in dedicated mode, including the allocation of dedicated channels.

An RR-session is always initiated by a mobile station through the access procedure, either for an outgoing call, or in response to a paging message. The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the mobile, and the paging sub-channel structure, are handled in the RR layer. In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

5.1.1 Handover

In a cellular network, the radio and fixed links required are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. The execution and measurements required for handover form one of basic functions of the RR layer.

There are four different types of handover in the GSM system, which involve transferring a call between:

- channels (time slots) in the same cell,
- cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
- cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and
- cells under the control of different MSCs.

The first two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signalling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. An important aspect of GSM is that the original MSC, the *anchor MSC*, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of another MSC, called the *relay MSC*.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on a metric [16] related to received signal strength. This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

The algorithm for when a handover decision should be taken is not specified in the GSM recommendations. There are two basic algorithms used, both closely tied in with power control. This is because the BSC usually does not know whether the poor signal quality is due to multipath fading or to the mobile having moved to another cell. This is especially true in small urban cells.

The 'minimum acceptable performance' algorithm [3] gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased. If further power increases do not improve the signal, then a handover is considered. This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.

The 'power budget' method [3] uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level. It thus gives precedence to handover over power control. It avoids the 'smeared' cell boundary problem and reduces co-channel interference, but it is quite complicated.

5.2 Mobility management

The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

5.2.1 Location updating

A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell. One possibility would be to page every cell in the network for each call, which is obviously a waste of radio bandwidth. At the other extreme, the mobile could notify the system, via location updating messages, of its current location at the individual cell level. This would require paging messages to be sent to only one cell, but would be very wasteful due to the large

number of location updating messages. A compromise solution used in GSM is to group cells into *location areas*. Updating messages are required only when moving between location areas, and mobile stations are paged in the cells of their current location area.

The location updating procedures, and subsequent call routing, use the MSC and the Home and Visitor location registers. When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location. In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number. The reason a routing number is not normally assigned, even though it would reduce signalling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls. If the subscriber is entitled to service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.

For reliability reasons, GSM also has a periodic location updating procedure. If an HLR or MSC/VLR fails, to have each mobile register simultaneously to bring the database up to date would cause overloading. Therefore, the database is updated as location updating events occur. The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signalling traffic and speed of recovery. If a mobile does not register after the updating time period, it is deregistered.

A procedure related to location updating is the IMSI attach and detach. A detach lets the network know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages. An attach is similar to a location update, and informs the system that the mobile is reachable again. The activation of IMSI attach/detach is up to the operator on an individual cell basis.

5.2.2 Authentication and security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be is a very important element of a mobile network. The problems being encountered by AMPS networks in the United States due to cloning of cellular phones makes the necessity of authentication painfully obvious. Authentication involves two functional entities: the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret subscriber key, one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjuction with the subscriber's key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated [16].

The same initial random number and subscriber key are also used to compute the ciphering key, using an algorithm called A8. This ciphering key, together with the TDMA frame number, are used by the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst (the two 57 bit blocks). Enciphering is an option for the fairly paranoid, since the signal is already digitally encoded, interleaved, and transmitted in bursts, thus providing protection from all but the most persistent and dedicated eavesdroppers. The A5 algorithm is unique and is given only to the signatories of the Memorandum of Understanding (MoU). The A3 and A8 algorithms are operator dependent.

Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber. As mentioned earlier, each GSM terminal is identified by a unique International Mobile Equipment Identity (IMEI) number. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

white-listed The terminal is allowed to connect to the network.

grey-listed The terminal is under observation from the network for possible problems.

black-listed The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

5.3 Communication management

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and Short Message Service management. Each of these may be considered as a separate sublayer within the CM layer.

Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

5.3.1 Call routing

Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which uses the ITU E.164 numbering plan. This number includes a country code and a National Destination Code which identifies the subscriber's operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. It should be noted that the GMSC function is distinct from the MSC function, but is usually implemented in an MSC in the home network, due to charging

considerations. The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which also uses the E.164 numbering plan. MSRNs are related to the geographical numbering plan, and are not permanently assigned to subscribers, nor are they visible to subscribers.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have an MSRN (see the location updating section). The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area (see Figure 4).

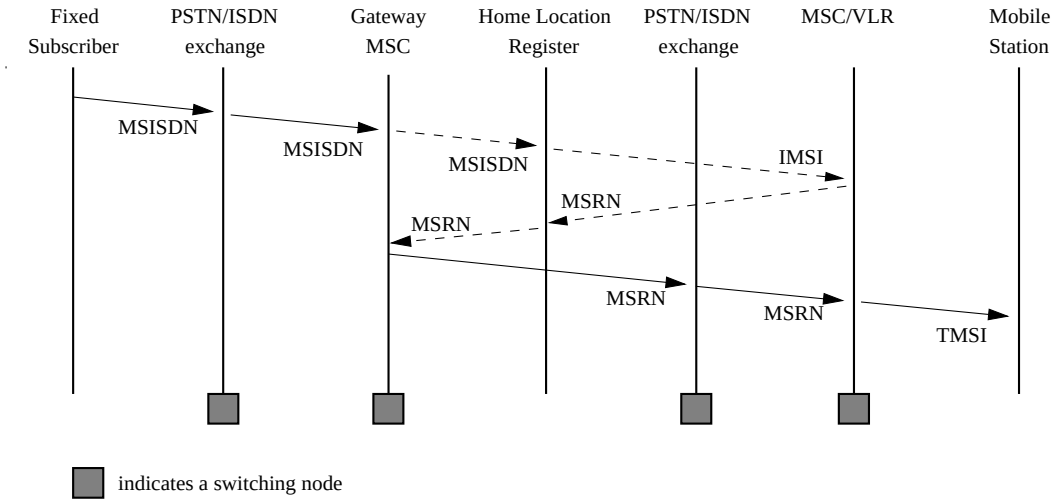


Figure 4: Call routing for a mobile terminating call

6 Conclusion and comments

In this paper I have tried to give an overview of the GSM system. As with any overview, and especially one covering a standard over 6000 pages long, there are many details missing. I hope I have given the general flavor of GSM and the philosophy behind its design. It was a monumental task that the original GSM committee undertook, and one that has proven a success, showing that international cooperation on such projects between academia, industry, and government can succeed. It is a standard that ensures interoperability without stifling competition and innovation among suppliers, to the benefit of the public both in terms of cost and quality of service. For example, by using Very Large Scale Integration (VLSI) microprocessor technology, many functions of the mobile station can be built on one chipset, resulting in lighter, more compact, and more energy-efficient terminals.

Telecommunications are evolving towards personal communication networks, whose objective can be stated as the availability of all communication services anytime, anywhere, to anyone, by a single identity number and a pocketable communication terminal [25]. Having a multitude of incompatible systems throughout the world moves us farther away from this ideal. The economies of scale created by a unified system are enough to justify its implementation, not to mention the convenience to people of carrying just one communication terminal anywhere they go, regardless of national boundaries.

The GSM system, and its relatives operating at 1800 MHz (DCS1800) and 1900 MHz (PCS1900), are the first approach at a true personal communication system. The SIM card is a novel approach that implements personal mobility in addition to terminal mobility. Together with international roaming, and support for a variety of services such as telephony, data transfer, fax, Short Message Service, and supplementary services, GSM comes close to fulfilling the requirements for a personal communication system: close enough that it is being used as a basis for the next generation of mobile communication technology in Europe, the Universal Mobile Telecommunication System (UMTS).

Another point where GSM has shown its commitment to openness, standards and interoperability

is the compatibility with the Integrated Services Digital Network (ISDN) that is evolving in most industrialized countries, and Europe in particular (the so-called Euro-ISDN). GSM is the first system to make extensive use of the Intelligent Networks concept, in in which services like 800 numbers are concentrated and handled from a few centralized service centers, instead of being distributed over every switch in the country. This is the concept behind the use of the various registers such as the HLR. In addition, the signalling between these functional entities uses Signalling System Number 7, an international standard already deployed in many countries and specified as the backbone signalling network for ISDN.

GSM is a very complex standard, but that is probably the price that must be paid to achieve the level of integrated service and quality offered while subject to the rather severe restrictions imposed by the radio environment.

References

[1] Jan A. Audestad. Network aspects of the GSM system. In *EUROCON 88*, June 1988.

[2] D. M. Balston. The pan-European system: GSM. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[3] David M. Balston. The pan-European cellular technology. In R.C.V. Macario, editor, *Personal and Mobile Radio Systems*. Peter Peregrinus, London, 1991.

[4] M. Bezler et al. GSM base station system. *Electrical Communication*, 2nd Quarter 1993.

[5] David Cheeseman. The pan-European cellular mobile radio system. In R.C.V. Macario, editor, *Personal and Mobile Radio Systems*. Peter Peregrinus, London, 1991.

[6] C. Déchaux and R. Scheller. What are GSM and DCS. *Electrical Communication*, 2nd Quarter 1993.

[7] M. Feldmann and J. P. Rissen. GSM network systems and overall system integration. *Electrical Communication*, 2nd Quarter 1993.

[8] John M. Griffiths. *ISDN Explained: Worldwide Network and Applications Technology*. John Wiley & Sons, Chichester, 2nd edition, 1992.

[9] I. Harris. Data in the GSM cellular network. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[10] I. Harris. Facsimile over cellular radio. In D. M. Balston and R.C.V. Macario, editors, *Cellular Radio Systems*. Artech House, Boston, 1993.

[11] Thomas Haug. Overview of the GSM project. In *EUROCON 88*, June 1988.

[12] Josef-Franz Huber. Advanced equipment for an advanced network. *Telcom Report International*, 15(3-4), 1992.

[13] Hans Lobensommer and Helmut Mahner. GSM – a European mobile radio standard for the world market. *Telcom Report International*, 15(3-4), 1992.

[14] Bernard J. T. Mallinder. Specification methodology applied to the GSM system. In *EUROCON 88*, June 1988.

[15] Seshadri Mohan and Ravi Jain. Two user location strategies for personal communication services. *IEEE Personal Communications*, 1(1), 1994.

[16] Michel Mouly and Marie-Bernadette Pautet. *The GSM System for Mobile Communications. published by the authors, 1992.*

[17] Jon E. Natvig, Stein Hansen, and Jorge de Brito. Speech processing in the pan-European digital mobile radio system (GSM) — system overview. In IEEE GLOBECOM 1989*, November 1989.*

[18] Torbjorn Nilsson. Toward a new era in mobile communications. http://193.78.100.33/ (Ericsson WWW server).

[19] Moe Rahnema. Overview of the GSM system and protocol architecture. IEEE Communications Magazine*, April 1993.*

[20] E. H. Schmid and M. Kähler. GSM operation and maintenance. Electrical Communication*, 2nd Quarter 1993.*

[21] Marko Silventoinen. Personal email, quoted from European Mobile Communications Business and Technology Report, March 1995.

[22] C. B. Southcott et al. Voice control of the pan-European digital mobile radio system. In IEEE GLOBECOM 1989*, November 1989.*

[23] P. Vary et al. Speech codec for the European mobile radio system. In IEEE GLOBECOM 1989*, November 1989.*

[24] C. Watson. Radio equipment for GSM. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems*. Artech House, Boston, 1993.*

[25] Robert G. Winch. Telecommunication Transmission Systems*. McGraw-Hill, New York, 1993.*