CHAPTER 5

Global System for Mobile Communications (GSM)

5.1 GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

GSM is much more than just an acronym for Global System for Mobile Communication. It signifies an extremely successful technology and bearer for mobile communication system. GSM today covers 71% of all the digital wireless market. The mobile telephone has graduated from being a status symbol to a useful appliance. People use it not only in business but also in personal life. Its principal use is for wireless telephony, and messaging through SMS. It also supports facsimile and data communication.

GSM is based on a set of standards, formulated in the early 1980s (see Table 5.1 for the GSM timeline). 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 mobile system, which was later rechristened as Global System for Mobile Communication. See Chapter 1 for cellular network evolution and standards. The proposed GSM system had to meet certain business objectives. These are:

- Support for international roaming.
- Good speech quality.
- Ability to support handheld terminals.
- Low terminal and service cost.
- Spectral efficiency.
- Support for a range of new services and facilities.
- ISDN compatibility.

Due to its innovative technologies and strengths, GSM rapidly became truly global. Many of the new standardization initiatives came from outside Europe. Depending on locally available frequency bands, different air interfaces were defined. Of these prominent ones are 900 MHz, 1800 MHz and 1900 MHz. However, architecture, protocols, signaling and roaming are identical in all networks independent of the operating frequency bands.

Table 5.1 GSM history timeline

Year	*Event*
1982	Groupe Spécial Mobile (GSM) established
1987	Essential elements of wireless transmission specified
1989	GSM becomes an ETSI technical committee
1990	Phase 1 GSM 900 specification (designed 1987 through 1990) frozen
1991	First GSM network launched
1993	First roaming agreement came into effect
1994	Data transmission capability launched
1995	Phase 2 launched. Fax and SMS roaming services offered
2002	SMS volume crosses 24 billion/year, 750 million subscribers

GSM uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access). See Section 3.2 for definition of these multiple access procedures. The GSM system has an allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band. Using FDMA, this band is divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is then further divided into eight time slots. Therefore, with the combination of FDMA and TDMA we can realize a maximum of 992 channels for transmitting and receiving. In order to be able to serve hundreds of thousands of users, the frequency must be reused. This is done through cells.

The frequency reuse concept led to the development of cellular technology as originally conceived by AT&T and Bell Labs way back in 1947. The essential characteristics of this reuse are as follows:

- The area to be covered is subdivided into radio zones or cells (Fig. 5.1). Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.
- Each cell i receives a subset of frequencies fbi from the total set assigned to the respective mobile network. To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.
- Only at a distance of D (known as frequency reuse distance), the same frequency from the set fbi can be reused. Cells with distance D from cell i, can be assigned one or all the frequencies from the set fbi belonging to cell i.
- When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.

The regular repetition of frequencies in cells result in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by k, the number of cells in the cluster. This also defines the frequency reuse distance D. Figure 5.1 shows an example of a cluster size of 4.

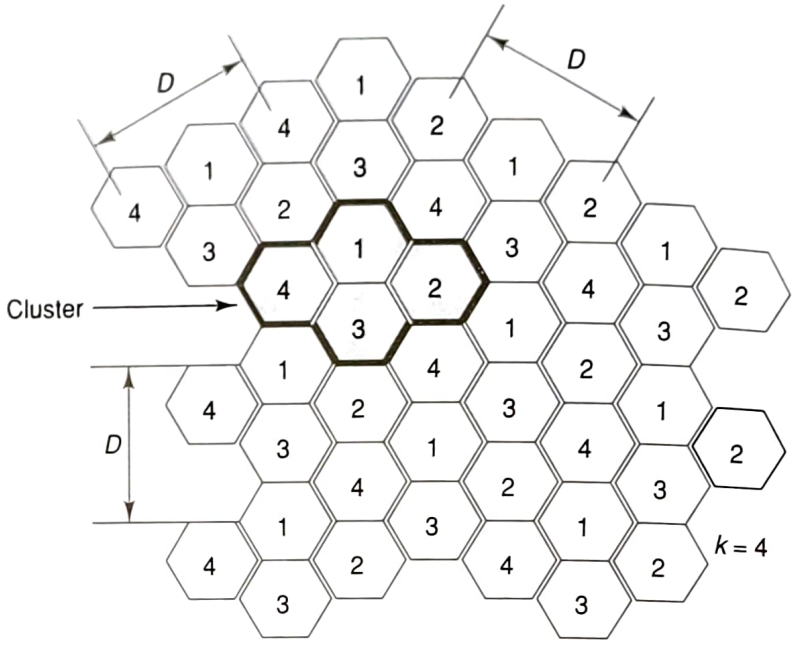


Figure 5.1 Cell Clusters in GSM

5.2 GSM ARCHITECTURE

GSM networks are structured in hierarchic fashion (Fig. 5.2). It consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre). The administrative region is commonly known as PLMN (Public Land Mobile Network). Each administrative region is subdivided into one or many Location Area (LA). One LA consists of many cell groups. Each cell group is assigned to one BSC (Base Station Controller). For each LA there will be at least one BSC. Cells in one BSC can belong to different LAs.

Cells are formed by the radio areas covered by a BTS (Base Transceiver Station) (Fig. 5.3). Several BTSs are controlled by one BSC. Traffic from the MS (Mobile Station) is routed through MSC. Calls originating from or terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway MSC). Figure 5.3 depicts the architecture of a GSM PLMN from technology point of view, whereas Figure 5.4 depicts the same architecture from the operational point of view.

For all subscribers registered with a cellular network operator, permanent data such as the service profile is stored in the Home Location Register (HLR). The data relate to the following information:

- Authentication information like International Mobile Subscriber Identity (IMSI).
- Identification information like name, address, etc., of the subscriber.
- Identification information like Mobile Subscriber ISDN (MSISDN), etc.
- Billing information like prepaid or postpaid customer.
- Operator selected denial of service to a subscriber.

- Handling of supplementary services like for CFU (Call Forwarding Unconditional), CFB (Call Forwarding Busy), CFNR (Call Forwarding Not Reachable) or CFNA (Call Forwarding Not Answered).

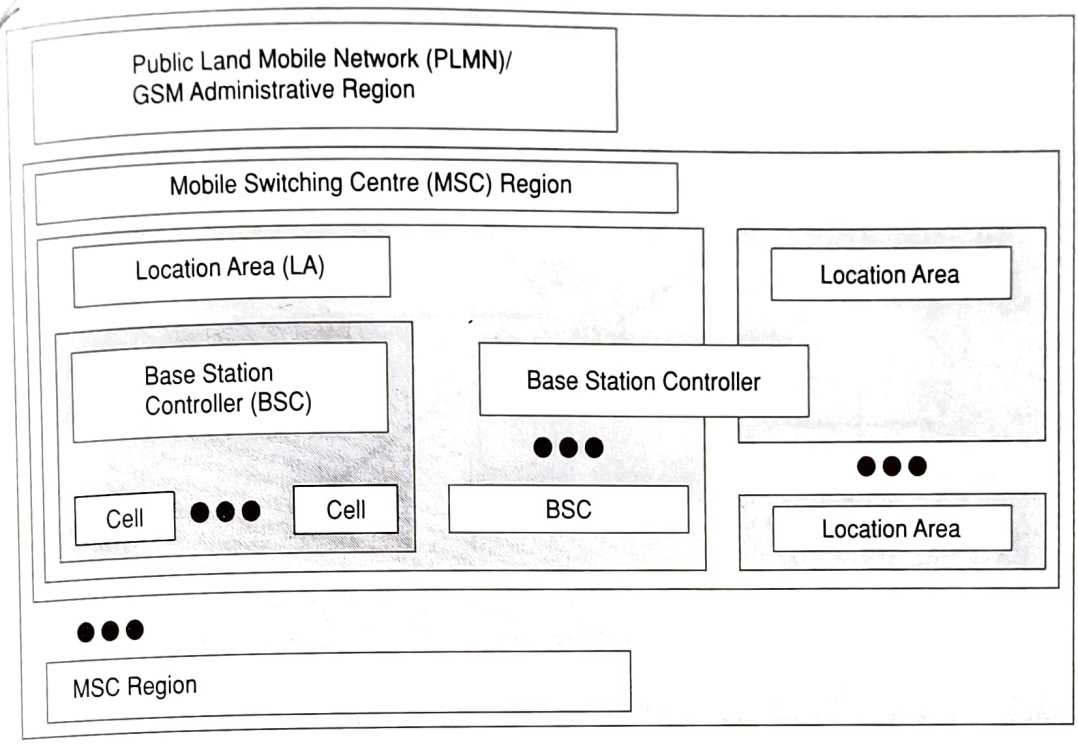


Figure 5.2 GSM System Hierarchy

- Storage of SMS Service Center (SC) number in case the mobile is not connectable so that whenever the mobile is connectable, a paging signal is sent to the SC.
- Provisioning information like whether long distance and international calls are allowed or not.
- Provisioning information like whether roaming is enabled or not.
- Information related to auxiliary services like Voice mail, data, fax services, etc.
- Information related to auxiliary services like CLI (Caller Line Identification), etc.
- Information related to supplementary services for call routing. In GSM network, one can customize the personal profile to the extent that while the subscriber is roaming in a foreign PLMN, incoming calls can be barred. Also, outgoing international calls can be barred, etc.

There is some variable information, which could also be part of the HLR. This includes the pointer to the VLR, location area of the subscriber, Power OFF status of the handset, etc.

5.3 GSM Entities

The GSM technical specifications define different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into five main groups (Fig. 5.4):

- It acts like a normal switching node for ISDN.
- It provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers and call routing.
- It includes databases needed in order to store information to manage the mobility of a roaming subscriber.

These different services are provided in conjunction with several functional entities, which together form the Network Subsystem. The signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7). SS7 is used for trunk signaling in ISDN and widely used in today's public networks. SS7 is also used for SMS, prepaid, roaming and other intelligent network functions.

The MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the call-routing and roaming capabilities of GSM. The HLR is considered a very important database that stores information of subscribers belonging to the covering area of a MSC. Although a HLR may be implemented as a distributed database, there is logically only one HLR per GSM network. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network. This includes information like current location of the mobile, all the service provisioning information and authentication data. When a phone is powered off, this information is stored in the HLR. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. HLR is always fixed and stored in the home network, whereas the VLR logically moves with the subscriber.

The VLR can be considered a temporary copy of some of the important information stored in the HLR. VLR is similar to a cache, whereas HLR is the persistent storage. The VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning of the subscribed services. This is true for each mobile currently located in the geographical area controlled by a VLR. GSM standards define interfaces to HLR; however, there is no interface standard for VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment implement the VLR as an integral part of the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR.

Note: MSC contains no information about a particular mobile station—this information is stored in location registers.

When a subscriber enters the covering area of a new MSC, the VLR associated with this MSC will request information about the new subscriber from its corresponding HLR in the home network. For example, if a subscriber of a GSM network in Bangalore is roaming in Delhi, the HLR data of the subscriber will remain in Bangalore with the home network, however, the VLR data will be copied to the roaming network in Delhi. The VLR will then have enough information in order to assure the subscribed services without needing to refer to the HLR each time a communication is established. Though the visiting network in Delhi will provide the services, the billing for the services will be done by the home network in Bangalore.

Within the NSS there is a component called Gateway MSC (GMSC) that is associated with the MSC. A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user and vice versa. The GMSC is often implemented in the same node as the MSC. Like the GMSC, there is another node called GIWU (GSM Interworking Unit). The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

these terminals are continuously decreasing. The life of a battery between charging is also increasing. The evolution of technologies allowed decrease of power requirement to less than 1 W.

The SIM is installed in every GSM phone and identifies the terminal. Without the SIM card, the terminal is not operational. The SIM cards used in GSM phones are smart processor cards. These cards possess a processor and a small memory. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. 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 security information. Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using his or her SIM card. The SIM card may be protected against unauthorized use by a password or personal identity number. Typically, SIM cards contain 32 K bytes of memory. Part of the memory in the SIM card is available to the user for storing address book and SMS messages. Applications are developed and stored in SIM cards using SAT (SIM Application Toolkit). SAT is something similar to Assembly languages of computers and is proprietary to the SIM vendor. Nowadays Java Smart cards are coming to the market. In Java Smart card, the applications are written in Java language and are portable across SIM cards from different vendors.

5.3.2 The Base Station Subsystem

The BSS (Base Station Subsystem) connects the Mobile Station and the NSS (Network and Switching Subsystem). It is in charge of the transmission and reception for the last mile. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or Base Station in short.
- The Base Station Controller (BSC).

The Base Transceiver Station corresponds to the transceivers and antennas used in each cell of the network. In a large urban area, a large number of BTSs are potentially deployed. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. The BTS houses the radio transmitter and the receivers that define a cell and handles the radio-link protocols with the Mobile Station. Each BTS has between one and 16 transceivers depending on the density of users in the cell.

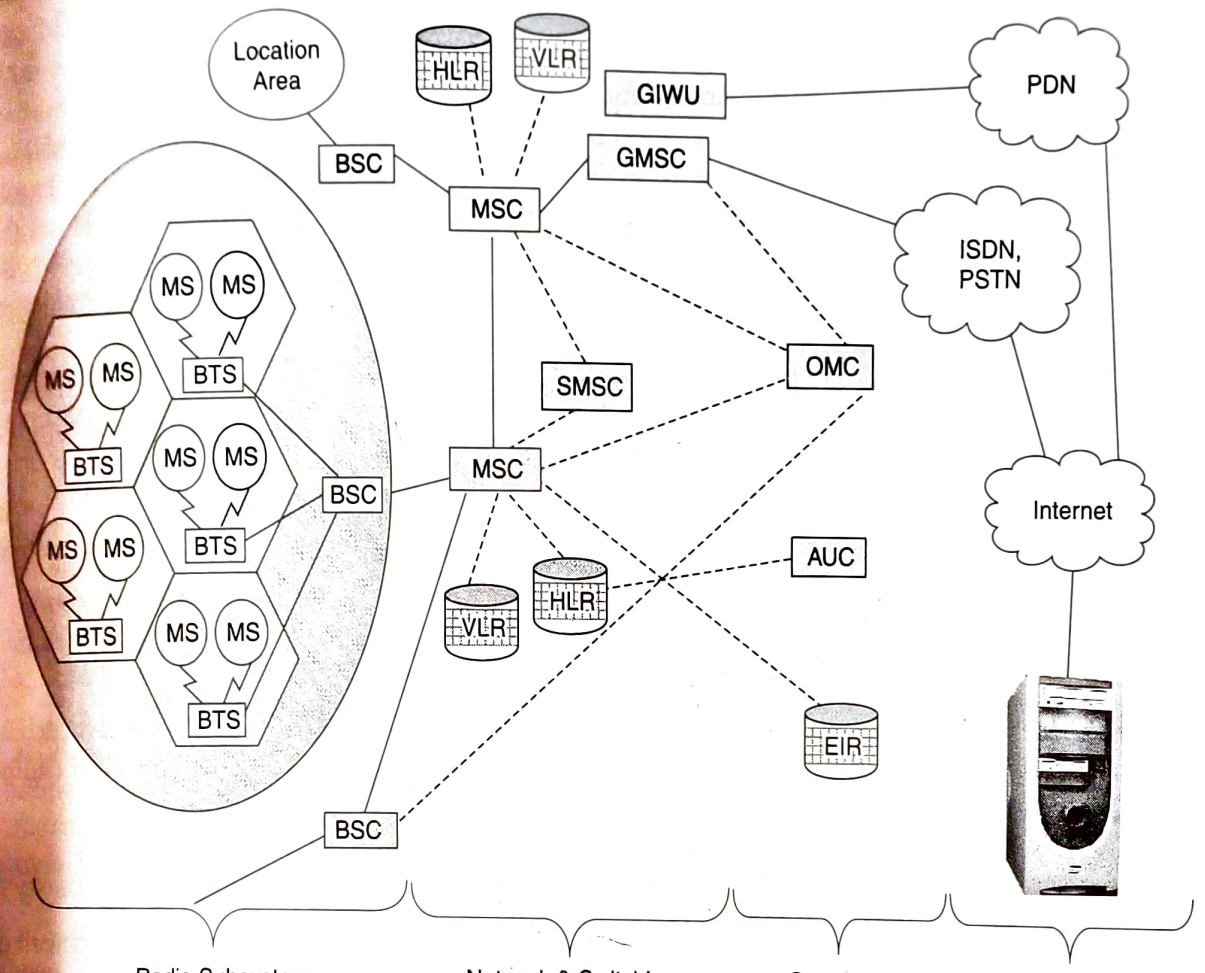
Base Station Controller is the connection between the BTS and the Mobile service Switching Center (MSC). The BSC manages the radio resources for one or more BTSs. It handles handovers, radio-channel setup, control of radio frequency power levels of the BTSs, exchange function, and frequency hopping.

5.3.3 The Network and Switching Subsystem

The central component of the Network Subsystem is the Mobile Switching Center (MSC). It does multiple functions. They are:

- It acts like a normal switching node for mobile subscribers of the same network (connection between mobile phone to mobile phone within the same network).
- It acts like a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone).

handheld terminals were quite big. Though the phones have become smaller and lighter, they are still called Mobile Stations. MS consists of two main elements:



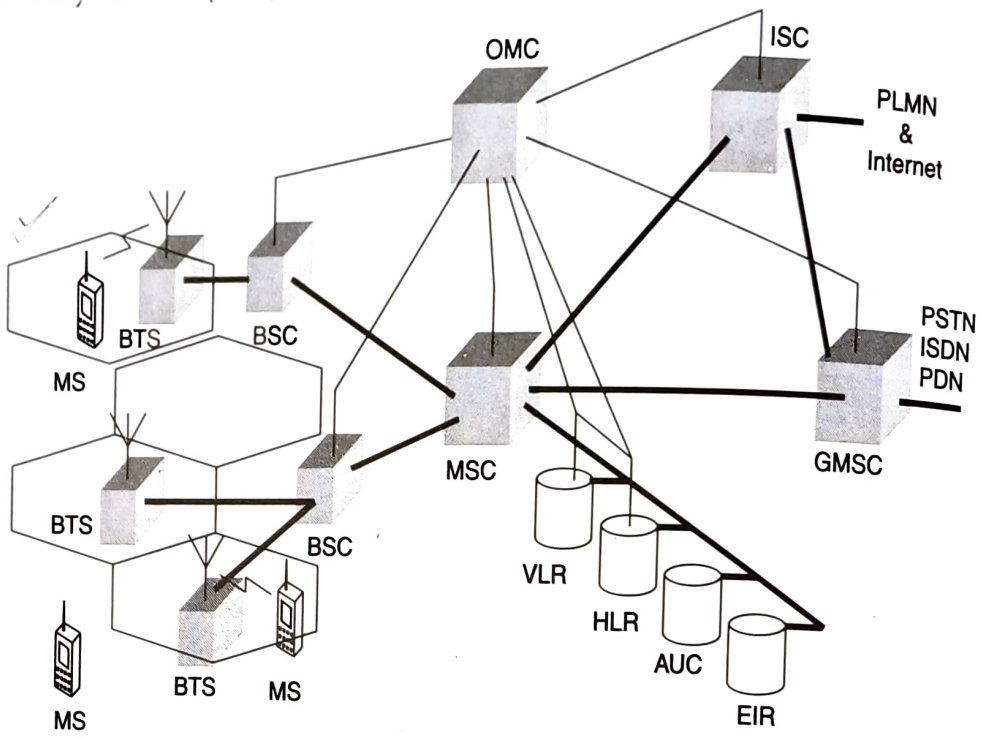
AUC	Authentication Center	MS	Mobile Station
BSC	Base Station Controller	MSC	Mobile Switching Center
BTS	Base Transceiver Station	OMC	Operation and Maintenance Center
EIR	Equipment Identity Register	PDN	Public Data Network
GIWU	Gateway Interworking Unit	PSTN	Public Switched Telephone Network
GMSC	Gateway MSC	SC	Service Center/SMS Controller
HLR	Home Location Register	SMSC	Short Message Service Center
ISDN	Integrated System Digital Network	VLR	Visitor Location Register

Figure 5.4 System Architecture of GSM

- The mobile equipment or the mobile device. In other words, this is a phone without the SIM card.
- The Subscriber Identity Module (SIM).

There are different types of terminals distinguished principally by their power and application. The handheld GSM terminals have experienced the highest evolution. The weight and volume of

- The Mobile Station (MS). This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).



AUC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
EIR	Equipment Identity Register
GMSC	Gateway MSC
HLR	Home Location Register
ISC	International Switching Center
ISDN	Integrated System Digital Network
MS	Mobile Station
MSC	Mobile Switching Center
OMC	Operation and Maintenance Center
PDN	Packet Data Network
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
VLR	Visitor Location Register

Figure 5.3 Architecture of GSM

- The Base Station Subsystem (BSS). This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
- The Network and Switching Subsystem (NSS). This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).
- The Operation and Support Subsystem (OSS). This includes the Operation and Maintenance Center (OMC).
- The data infrastructure that includes Public Switched Telephone Network (PSTN), Integrated System Digital Network (ISDN), and the Public Data Network (PDN).

5.3.1 Mobile Station

Mobile Station is the technical name of the mobile or the cellular phone. In early days mobile phones were a little bulky and were sometimes installed in cars like other equipment. Even the

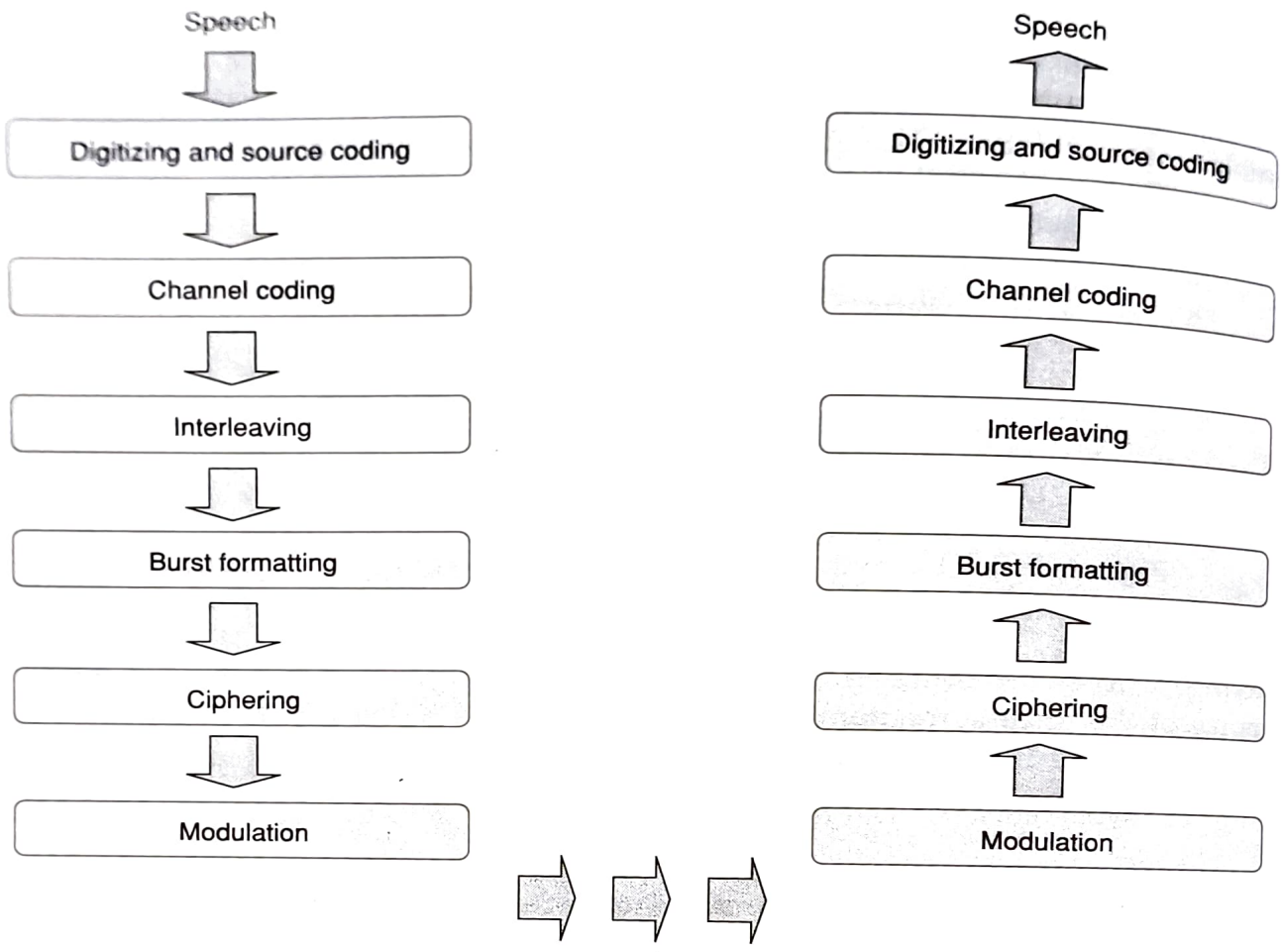


Figure 5.6 Sequence of Operation from Speech to Radio Wave

The mobile station can be anywhere within a cell. Also, the distance between the base station and the mobile station vary. Due to mobility of the subscriber, the propagation time between the base station and the mobile keeps varying. When a mobile station moves further away, the burst transmitted by this mobile may overlap with the time slot of the adjacent time slot. To avoid such collisions, the Timing Advance technique is used. In this technique, the frame is advanced in time so that this offsets the delay due to greater distance. Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

5.4.1 An Example

In this section let us take an example of how and what happens within the GSM network when someone from a fixed network calls someone in a GSM network. Let us assume that the called party dialed a GSM directory number +919845052534. Figure 5.7 depicts the steps for this call processing.

is then represented in signed 13-bit linear PCM value. This digitized data is passed to the coder with frames of 160 samples. The encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec.

Channel coding: This step introduces redundancy information into the data for error detection and possible error correction. The gross bit rate after channel coding is 22.8 kbps (or 456 bits every 20 ms). These 456 bits are divided into eight 57-bit blocks, and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors.

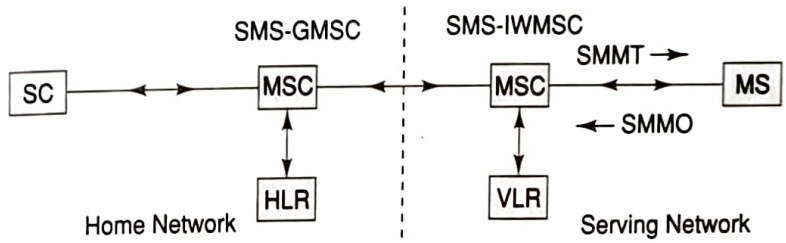


Figure 5.5 The Network Structure for the Short Message Transfer

Interleaving: This step rearranges a group of bits in a particular way. This is to improve the performance of the error-correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors.

Ciphering: Encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS.

Burst formatting: Adds some binary information to the ciphered block. This additional information is used for synchronization and equalization of the received data.

Modulation: The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK). Using this technique the binary data is converted back into analog signal to fit the frequency and time requirements for the multiple access rules. This signal is then radiated as radio wave over the air. Each time slot burst is 156.25 bits and contains two 57-bit blocks, and a 26-bit training sequence used for equalization (Fig. 5.6). A burst is transmitted in 0.577 ms for a total bit rate of 270.8 Kbps.

Multipath and equalization: At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So not only is the "right" signal (the output signal of the emitter) received by an antenna, but many reflected signals, which corrupt the information, with different phases are also received. An equaliser is in charge of extracting the "right" signal from the received signal. It estimates the channel impulse response of the GSM system and then constructs an inverse filter. In order to extract the "right" signal, the received signal is passed through the inverse filter.

Synchronization: For successful operation of a mobile radio system, time and frequency synchronization are needed. Frequency synchronization is necessary so that the transmitter and receiver frequency match (in FDMA). Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA).

5.3.4 The Operation and Support Subsystem (OSS)

As the name suggests, Operations and Support Subsystem (OSS) controls and monitors the GSM system. The OSS is connected to different components of the NSS and to the BSC. It is also in charge of controlling the traffic load of the BSS. However, the increasing number of base stations due to the development of cellular radio networks, has resulted in some of the maintenance tasks being transferred to the BTS. This transfer decreases considerably the costs of maintenance of the system. Provisioning information for different services is managed in this subsystem.

Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). EIR contains a list of IMEIs of all valid terminals. An IMEI is marked as invalid if it has been reported stolen or is not type approved. The EIR allows the MSC to forbid calls from this stolen or unauthorized terminals.

Authentication Center (AUC) is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key stored in each subscriber's SIM card. These data help to verify the user's identity.

5.3.5 Message Centre

Short Message Service or SMS is one of the most popular services within GSM. SMS is a data service and allows a user to enter text message up to 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characters (some European alphabets or binary data) are used, and 70 characters in length when non-Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16-bit Unicode). SMS is a proactive bearer and is an always ON network. Message center is also referred to as Service Centre (SC) or SMS Controller (SMSC). SMSC is a system within the core GSM network, which works as a store and forward system for SMS messages. Refer to Figure 5.5 for SMS architecture.

There are two types of SMS, SMMT (Short Message Mobile Terminated Point-to-Point), and SMMO (Short Message Mobile Originated Point-to-Point). SMMT is an incoming short message from the network and is terminated in the MS (phone or Mobile Station). SMMO is an outgoing message, originated in the MS, and forwarded to the network for delivery. For an outgoing message, the SMS is sent from the phone to SC via the VLR and the Interworking MSC (IWMSC). For incoming SMS message the path is from SC to the MS via the HLR and the Gateway MSC (GMSC). Please see Chapter 6 for SMS and related technologies.

5.4 Call Routing in GSM

Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital fashion. In GSM there are many complex technologies used between the human analog interface in the mobile and the digital network (Fig. 5.6).

Digitizer and source coding: The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop. In this technique, information from previous samples is used to predict the current sample. Each sample

digits of operator code, followed by one decimal digit level number with a five decimal digit subscriber number. In India, a MSISDN number looks like 919845062050. In this number 91 is the CC, 98 is the NDC, and 45062050 is the SN. In India, the SN is subdivided into operator code and subscriber code (45 is the operator code and 062050 is the subscriber code). Sometimes subscriber code is also subdivided into one digit level number (0 in this case) followed by five digit subscriber ID (62050).

- *Location Area Identity:* Each LA in a PLMN has its own identifier. The Location Area Identifier (LAI) is structured hierarchically and unique. LAI consists of three digits of CC, two digits of Mobile Network Code and maximum five digits of Location Area Code.
- *Mobile Station Roaming Number (MSRN):* When a subscriber is roaming in another network a temporary ISDN number is assigned to the subscriber. This ISDN number is assigned by the local VLR in charge of the mobile station. The MSRN has the same structure as the MSISDN.
- *Temporary Mobile Subscriber Identity (TMSI):* This a temporary identifier assigned by the serving VLR. It is used in place of the IMSI for identification and addressing of the mobile station. TMSI is assigned during the presence of the mobile station in a VLR and can change (ID hopping). Thus, it is difficult to determine the identity of the subscriber by listening to the radio channel. The TMSI is never stored in the HLR. However, it is stored in the SIM card. Together with the current location area, a TMSI allows a subscriber to be identified uniquely. For an ongoing communication the IMSI is replaced by the 2-tuple LAI, TMSI code.
- *Local Mobile Subscriber Identity (LMSI):* This is assigned by the VLR and also stored in the HLR. This is used as a searching key for faster database access within the VLR.
- *Cell Identifier:* Within a LA, every cell has a unique Cell Identifier (CI). Together with a LAI a cell can be identified uniquely through Global Cell Identity (LAI+CI).
- *Identification of MSCs and Location Registers:* MSCs, Location Registers (HLR, VLR), SCs are addressed with ISDN numbers. In addition, they may have a Signaling Point Code (SPC) within a PLMN. These point codes can be used to address these nodes uniquely within the Signaling System number 7 (SS#7) network.

5.7 Network Aspects in GSM

Transmission of voice and data over the radio link is only a part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally. This requires that registration, authentication, call routing and location updating functions are standardized across GSM networks. The geographical area covered by a network is divided into cells of small radius. When a call is in progress and the user is on the move, there will be a handover mechanism from one cell to another. This is like a relay race where one athlete passes on the baton to another. Though both roaming and handover functions are the basic characteristic of mobility, there is a difference between these functions. These functions are performed by the Network Subsystem, mainly using the Mobile Application Part (MAP) built on top of the Signalling System # 7 (SS7) protocol (Fig. 5.9).

microwave or leased lines. Any data related to user call (connection, teardown, etc.) are processed with SS7 protocol for signaling using ISUP (ISDN User Part) stack between network nodes. For mobile specific signaling a protocol stack called MAP (Mobile Application Part) is used over the SS7 network. All database transactions (enquiries, updates, etc.) and handover/roaming transactions between the MSC are performed with the help of MAP. For this purpose, each MSC uses registers known as SP (Signaling Point). These SPs are addressable through a unique code called Signaling Point Code (SPC). Signaling between MSC and BSS uses Base Station System Application Part (BSSAP) over SS7. Within BSS and at the air interface, signaling is GSM proprietary and does not use SS7.

5.6 GSM Addresses and Identifiers

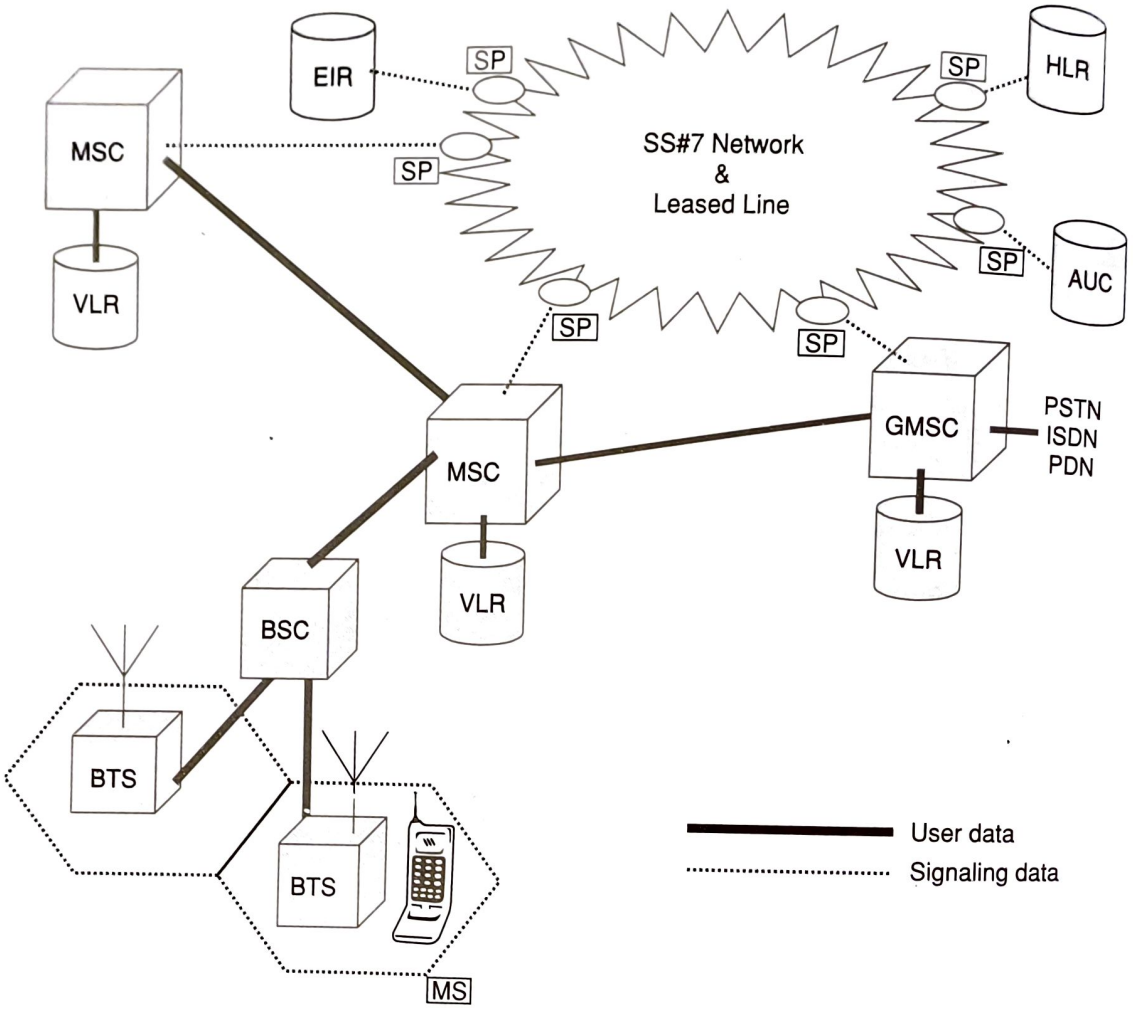
GSM distinguishes explicitly between the user and the equipment. It also distinguishes between the subscriber identity and the telephone number. To manage all the complex functions, GSM deals with many addresses and identifiers. They are:

- *International Mobile Station Equipment Identity (IMEI):* Every mobile equipment in this world has a unique identifier. This identifier is called IMEI. The IMEI is allocated by the equipment manufacturer and registered by the network operator in the Equipment Identity Register (EIR). In your mobile handset you can type *#06# and see the IMEI.
- *International Mobile Subscriber Identity (IMSI):* When registered with a GSM operator, each subscriber is assigned a unique identifier. The IMSI is stored in the SIM card and secured by the operator. A mobile station can only be operated when it has a valid IMSI. The IMSI consists of several parts. These are:
  - ❑ Three decimal digits of Mobile Country Code (MCC). For India the MCC is 404.
  - ❑ Two decimal digits of Mobile Network Code (MNC). This uniquely identifies a mobile operator within a country. For Airtel in Delhi this code is 10.
  - ❑ Maximum 10 decimal digits of Mobile Subscriber Identification Number (MSIN). This is a unique number of the subscriber within the home network.
- *Mobile Subscriber ISDN Numbers (MSISDN):* The MSISDN number is the real telephone number as is known to the external world. MSISDN number is public information, whereas IMSI is private to the operator. This is a number published and known to everybody. In GSM a mobile station can have multiple MSISDN numbers. When a subscriber opts for fax and data, he is assigned a total of three numbers: one for voice call, one for fax call and another for data call. The MSISDN categories follow the international ISDN (Integrated Systems Data Network) numbering plan as the following:
  - ❑ Country Code (CC): One to three decimal digits of country code.
  - ❑ National Destination Code (NDC): Typically 2 to 3 decimal digits.
  - ❑ Subscriber Number (SN): Maximum 10 decimal digits.

The CC is standardized by the ITU-T through the E.164 standard. There are CCs with one, two, or three digits. For example, the CC for USA is 1, for India it is 91, and for Finland it is 358.The national regulatory authority assigns the NDC. In India it is 94 for BSNL and 98 for all other operators. In India the subscriber number SN is eight decimal digits. SN consists of two decimal

5.5 PLMN Interfaces

The basic configuration of a GSM network contains a central HLR and a central VLR. HLR contains all security, provisioning and subscriber-related information. VLR stores the location information and other transient data. MSC needs subscriber parameter for successful call set-up. Figure 5.8 shows a basic configuration of a GSM mobile communication network.



AUC	Authentication Center	ISDN	Integrated System Digital Network
BSC	Base Station Controller	MS	Mobile Station
BTS	Base Transceiver Station	MSC	Mobile Switching Center
EIR	Equipment Identity Register	PDN	Public Data Network
GMSC	Gateway MSC	PSTN	Public Switched Telephone Network
HLR	Home Location Register	SP	Signaling Point
		VLR	Visitor Location Register

Figure 5.8 Configuration of a GSM PLMN

Within the switching and management system, the transmission rate is 2 Mbits/s. This 2 Mbits/ interface is called E1 interface in India and in Europe. These are realized typically through

The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the 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. For example, the MSISDN number of a subscriber in Bangalore associated with Airtel network is +919845XYYYYY. This is a unique number and understood from anywhere in the world. In this example + means the prefix for international dialing like 00 in UK/India or 011 in USA. 91 is the country code for India (404 as defined in GSM). 45 is the network operator's code (Airtel in this case). X is the level number managed by the network operator ranging from 0 to 9. YYYYY is the subscriber code managed by the operator as well.

The call first goes to the local PSTN exchange. The PSTN exchange looks at the routing table and determines that it is a call to a mobile network. It forwards the call to the Gateway MSC (GMSC) of the mobile network. The MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If the user has not paid the bills, the call may not be routed. If the phone is powered off, a message may be played or forwarded to the voice mail. However, if MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present. If the VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location Area (LA). Within the LA it will page and locate the phone and connect the call.

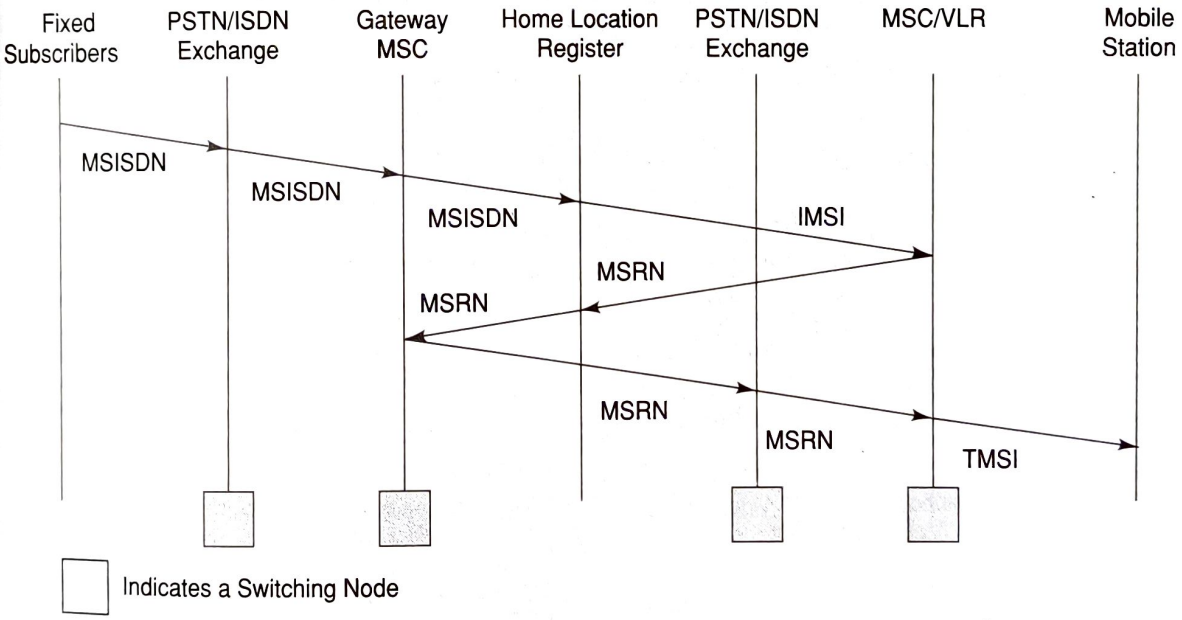


Figure 5.7 Call Routing for a Mobile Terminating Call

The first two types of handover, called internal handovers, involve only one BSC. To save SS7 signaling bandwidth, they are managed by the BSC without involving the MSC, except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSC. In order to determine whether a handover is required, due to RF criteria, the mobile shall take radio measurements from neighboring cells. These measurements are reported to the serving cell to determine a need for a handover. Additionally, the handover decision by the network may take into account both the measurement results from the MS and network directed criteria. The same decision process is used to determine when to perform both the intra-MSC and inter-MSC handover.

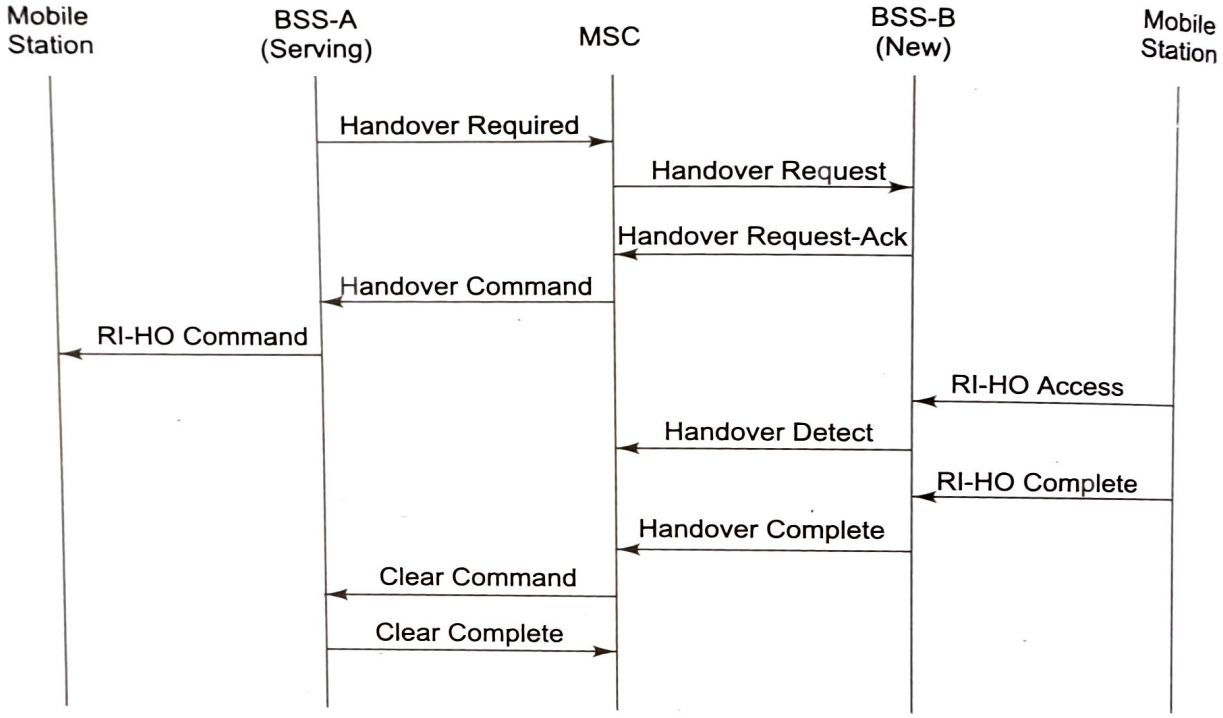


Figure 5.10 Handover Procedure

Figure 5.10 illustrates the handover procedure in GSM. The currently serving BSS sends a Handover_Required message to the MSC; the MSC sends a Handover_Request message to the new BSS from which it requires radio resources. This message contains details of the resource that is required. The message may also specify the channel in use. On receipt of this message the new BSS shall choose a suitable idle radio resource. This information is passed by the new BSS to the MS through MSC and old BSS using Handover_Request_Acknowledgement, Handover_Command, and Radio_Interface_Handover_Command respectively. The MS changes its association from the old BSS to the new BSS with a Handover_Access burst which contains the received handover reference number. The new BSS checks the handover reference number to ensure that it is the same as expected, and that there is a high probability that the correct MS has been captured. When the MS is successfully in communication with the network, i.e., the Radio Resource (RR) message Handover_Complete has been received from the MS, then the new BSS will immediately send a BSSMAP message Handover_Complete to the MSC and terminate the

When an MS is powered-off, the HLR is updated with an explicit IMSI detach. IMSI detach is equivalent to HLR data for the particular IMSI being unavailable; in this case logically the MS is not available and a connection cannot be established. However, the MS may be powered-on but may not be successfully connected to the network for an operator defined interval; this could be due to MS being out of coverage area—in such a case an implicit IMSI detach occurs.

To complete a call, IMSI must stay attached with a VLR and HLR. IMSI attach is accomplished through location updates. Location update can be initiated by either MS or the network. Frequent location update costs in terms of power in the MS and the SS7 signalling traffic; therefore, location update is restricted to the following conditions:

- When there is a mobile originated outgoing call, the location information is updated in the VLR and the HLR.
- When the MS moves from one Location Area (LA) to another LA the location information in the VLR and the HLR is updated. In Figure 5.2, we illustrated the hierarchical GSM networks with at least one administrative region, which is assigned to an MSC. Each administrative region is made up of multiple location area (LA) and each location area consists of several cell groups.
- The MS updates the location co-ordinates when its location is more than "k" cells away in distance from the location information of the last update.
- The MS updates the location information when it crosses exactly "k" cell boundaries irrespective of the distance.
- In addition, there is an explicit periodic location update by the MS. This time period is defined by the GSM network operator and is within the range of 1 deci-hour (6 minutes) to 240 deci-hours (24 hours) with a granularity of 1 deci-hour.

5.8.3 Handover

In a cellular network, while a call is in progress, the relationship between radio signal and the user is dynamic. User movements may make a user move away from a wireless tower, causing the radio signal strength to reduce, and ultimately break. Therefore, the user needs to be moved to another cell where the signal strength is higher. This will result in changing the association of resources to another channel within the same cell or a different cell altogether. This procedure of changing the resources is called handover. The handover needs to be very fast without any disruption to the service at the higher layer. This handover procedure is called "handoff" in North America. The handover can be initiated either by the MS or the network. A mobile initiated handover is based on radio subsystem criteria of Radio Frequency (RF) level, quality of the radio signal, or the distance from the tower; whereas, the network initiated handover that is assisted by a mobile device is based on the current traffic loading per cell, maintenance requests, etc.

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 (BTS) under the control of the same BSC.
- Cells under the control of different BSCs, but belonging to the same MSC.
- Cells under the control of different MSCs.

Management (MM) solves all these challenges. Using MM one can make outgoing calls and receive incoming calls while in motion; even at the vehicular state where the speed is higher than 60 kmph. The MM function handles all functions that arise from the mobility of the subscriber.

In a wired network where the device is stationary, the point of attachment to the network is fixed; here, address of the device is sufficient to locate the device in the routing table and establish a connection. However, in a wireless or mobile environment the point of attachment constantly changes, the device moves from one location to another location making the old routing table invalid; therefore, establishing and maintaining a connection is complex. As long as there is a wireless network with available channels, mobile originated outgoing calls are relatively easy to handle; for mobile terminated incoming calls, however, Paging and Location Updates are necessary. Also, Handover and Roaming are two important aspects in mobility. We will discuss mobility management in the following sections.

5.8.1 Paging

For a mobile terminated call, the MS needs to be traced, located, and then the call connected. The MS is traced through the Paging process within a location. Using the BSS signaling channel the Paging message for an MS is sent that includes the IMSI as the identifier of the MS. The message may also include an indication of which combination of channels will be needed for the subsequent transaction related to the paging. A single paging message across the MSC to BSS interface contains information of the cells in which the page shall be broadcast.

In Paging, the most difficult part of the decision is—which cell to start the paging from; because a cellular network may be spread over thousands of square-kilometres with thousands of cells. If we cannot locate the mobile quickly, the call cannot be connected resulting in lost revenue. For example, it can start at the center of the network and keep on searching each and every cell for a long time. However, such global paging is very expensive in terms of backbone and radio signaling channels. Also, global paging will take enormous amount of time. To optimize the cost and response time, paging starts at the location where the MS was present last. The location of the MS is recorded in the HLR and updated through Location Update. The MS is searched in these cells where it has the highest probability of being present. There are various algorithms for paging so that the MS can be located quickly with minimum effort and cost.

5.8.2 Location Update

Location update is concerned with the procedures that enable the network to know the current location of a powered-on MS so that the mobile terminated call routing can be completed. If the location of the MS is not known, tracking the MS through paging costs in terms of radio and backbone SS7 signalling (see Chapter 11) bandwidth. To optimize this, location information is regularly updated within the core network. Through location update, the presence and location information is kept up-to-date within the VLR and the HLR. Presence deals with willingness and availability of an MS for communication. Assuming that the MS is willing to communicate, the MS must be powered-on and attached to the network. If the MS is attached to the network, it must be located through Paging before a successful communication can take place for mobile terminated calls and mobile terminated SMS.

The signaling protocol in GSM is structured into three general layers, depending on the interface, as shown in Figure 5.9. Layer 1 is the physical layer, which uses the channel structures over the air interface. 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 or X.25, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of Signaling System Number 7 is used. Layer 3 of the GSM signaling protocol is itself divided into three sublayers.

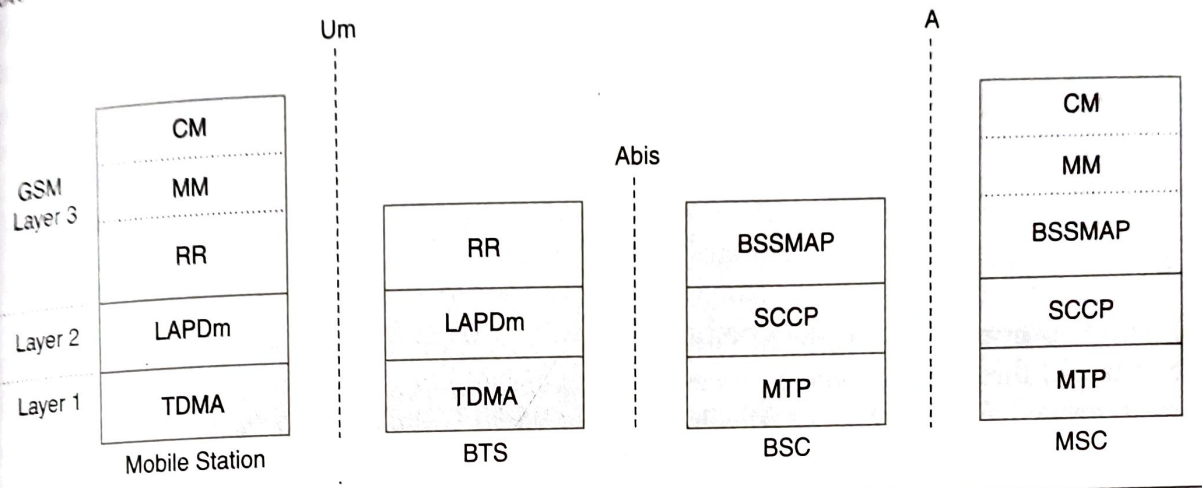


Figure 5.9 Signaling Protocol Structure in GSM

- *Radio Resources Management:* Controls the set-up, 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.

Signaling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished through the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of SS7). SS7 is also used for many other Intelligent Network services within the GSM. The specification of the MAP is quite complex, and at over 500 pages, it is one of the longest documents in the GSM recommendations.

5.8 Mobility Management

Think about a world in 1970s—a person traveling by train without having a GSM mobile phone or wireless communication device. If he wants to talk to someone (call the doctor, for example, for some critical healthcare help) or someone wants to talk (incoming call) to this person—how can this conversation take place? If the train stops at a station for a long duration, the person could try to locate a public call office in the station and make the call; but he must finish the call before the train departs. Unfortunately there was no way for someone to call this person (incoming call). Mobility

Let us now look at a completely different scenario where both the caller and the called party are roaming in a foreign network. Let us assume that two subscribers 'A' and 'B' from Airtel Bangalore are visiting Kolkata. When 'A' calls 'B', 'A' dials the number of 'B' which is a Bangalore number. Therefore, the call will be routed to Airtel in Bangalore. In Bangalore it is found that 'B' is roaming in Kolkata, therefore the call will be routed back to Kolkata. If you notice, though both subscribers are in Kolkata, the call is routed through Bangalore and both of them pay the long distance charges. To avoid this, some network operators came up with something called Optimal Call Routing (OCR). OCR will work only when the called party's VLR and the calling party's VLR are within the same MSC/VLR. Let us take the previous example and assume that both 'A' and 'B' are roaming at Kolkata's Airtel network. While 'A' makes a call to 'B', he prefixes a # in front of the number like #09845050505. This being an outgoing call, the Airtel MSC in Kolkata will look at the Kolkata VLR first. As the number is prefixed with #, it assumes that the other number is roaming in the same network as well. Therefore it looks at its own VLR once again to see whether 'B' is available in its database. If yes, it routes internally without forwarding the call to the home network. In case of 'B', though it is an incoming call, it is routed directly through the VLR without referring to the HLR at Bangalore.

5.9 GSM Frequency Allocation

GSM in general uses 900 MHz band; out of this, 890-915 MHz are allocated for the uplink (mobile station to base station) and 935–960 MHz for the downlink (base station to mobile station). Each way the bandwidth for the GSM system is 25 MHz (Fig. 5.12), which provides 125 carriers uplink/downlink each having a bandwidth of 200 kHz. The ARFCN (Absolute radio frequency channel numbers) denotes a forward and reverse channel pair which is separated in frequency by 45 MHz.

Mobile-to-base: $Ft(n) = 890.2 + 0.2(n-1)$ MHz

Base-to-mobile: $Ft(n) = Fr(n) + 45$ MHz

In practical implementation, a guard band of 100 kHz is provided at the upper and lower end of the GSM 900MHz spectrum, and only 124 (duplex) channels are implemented. Since 1995, new bands have been added to the basic 900MHz GSM. These bands are 1800 MHz and 1900MHz. 1800MHz band is licensed to the fourth GSM operator in India. The 1800 MHz band uses 1710–1785MHz and 1805–1880MHz (three times as much as primary 900MHz) with a total of 374 duplex channels. GSM 900 uses the four-cell repeat pattern for the frequency reuse cell sets. In most cases, each cell is divided into 120 degree sectors, with three base transceiver subsystems in each cell. Each base transceiver has a 120 degree antenna. These 12 sectors (called cells in GSM system) share the 124 channels.

To share the bandwidth for multiple users, GSM uses a combination of Time-Division Multiple Access (TDMA) and Frequency-Division Multiple Access (FDMA) encoding. 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 approximately 0.577 ms. Eight burst periods are grouped into a TDMA frame for approximately 4.615 ms, which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame. Channels are defined by the number and

defined in the E.164 numbering plan that includes CC (Country Code), NDC (National Destination Code), and SN (Subscriber Number) (Fig. 5.7).

MSRN is a temporary location-dependent MSISDN number. It is assigned by the serving VLR for each MS in its area. MSRNs are numbers reserved by a PLMN only for roaming use; and, not assigned to subscribers, nor are they visible to subscribers. The allocation of MSRN is done in such a fashion that the currently responsible MSC in the visited network (CC+NDC) can do routing of the call quite easily.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN (Fig. 5.7). The HLR typically stores only the SS7 address of the subscriber's current VLR. The VLR temporarily allocates 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. As a rule of thumb, HLR is referred for incoming call; whereas VLR is referred for outgoing call.

Roaming is of two types. These are:

- *Horizontal Roaming:* Horizontal roaming is between two networks from same family. For example, GSM to GSM roaming or GSM to UMTS roaming will be considered horizontal roaming.
- *Vertical Roaming:* Vertical roaming is between two networks from different families. For example, GSM to CDMA roaming or GPRS to WiFi will be considered vertical roaming. When vertical roaming happens without any disruption of session or service, it is called Seamless Roaming.

5.8.6 Roaming Example

Let us assume that the user's mobile number is +919844012345. This is a number in Spice network in Bangalore. The mobile subscriber is roaming in Mumbai. Somebody from a fixed phone in Mumbai wants to talk to this Spice subscriber. The caller (also known as 'A' party) dials 09844012345 from Mumbai. This call will be switched at the PSTN network in Mumbai and will be routed to Spice network in Bangalore. The Spice MSC will look at the HLR and know that the subscriber (called 'B' party) is now within the coverage of a mobile operator (Vodafone) in Mumbai—this is done using the MSRN. The call will be routed to the Mumbai MSC at Vodafone. The Vodafone MSC at Mumbai will look at its VLR to locate the Spice subscriber and route the call. Also, when the call is over, the charging information will be forwarded to the Spice network. Please note that for the incoming call, the routing always happens via the home network resulting in the call routing from Mumbai PSTN to Bangalore PLMN to Mumbai PLMN. The calling party (person in Mumbai) pays long distance tariff for Mumbai PSTN to Bangalore PLMN; the called party (Spice subscriber) pays for Bangalore PLMN to Mumbai PLMN long distance tariff in addition to roaming airtime charges. For outgoing call, the home network is not referred (other than the first time authentication), resulting in the call being directly routed by the visiting network. Let us consider the opposite scenario; the Spice subscriber from Bangalore is still roaming in Mumbai and wants to call someone in Mumbai. The Spice subscriber dials the Mumbai number, the Vodafone MSC looks at the VLR and routes the call directly to the Mumbai number. In this case, the Spice subscriber pays a local Mumbai to Mumbai call charge in addition to the airtime charges.

Figure 5.11 illustrates the normal location updating procedure with all elements pertaining to security functions, i.e., TMSI (Temporary Mobile Subscriber Identity) management, authentication and K_c management. Here it is assumed that during the handover the MSC/VLR is changed from old VLRo to new VLRn. During the Location Update the MS sends the LAI (Location Area Identifier) and the old TMSIo to the old VLRo. The VLRo sends the series of challenges RAND (1, ...n), and their respective answers SRES (1, ...n) of challenges, and the respective ciphering keys Kc (1, ...n) with the IMSI of the MS. VLRo receives all these RAND challenges from the HPLMN (Home Public Land Mobile Network). If the authentication is successful, the HLR is updated with new location; the ciphering starts with new Kc and a new TMSI is allocated. As part of housekeeping, the new VLRn is registered in the HLR; the HLR also informs the VLRo to de-register the IMSI. The VLRo deletes all entries related to this IMSI including the TMSIo.

5.8.5 Roaming

Handover relates to moving from one point of attachment to another point of attachment within the same network operator; when this movement happens between two different networks it is called roaming. Different networks imply two separate billing and charging domains.

When a mobile station is powered-off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected. When a mobile station is switched on in a new network (for example, the user has disembarked from an aircraft in a new country) or the subscriber moves to a different operator's PLMN (Public Land Mobile Network), the subscriber must register with the new network to indicate its current location. The first location update procedure is called the IMSI attach procedure where the MS indicates its IMSI to the new network. Normally, 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. If the mobile station is authenticated and authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR. A location update is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

Roaming is a killer application in GSM that allows users to seamlessly move around nationally and internationally and remain connected. Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, GSM allows roaming around the world. When there is an incoming call for a subscriber, the mobile phone needs to be located, a channel needs to be allocated and the call connected. A powered-on mobile is informed of an incoming call by a paging message sent over the paging channel of the cells within the current location area. The location updating procedures, and subsequent call routing, use the MSC and both HLR and the VLR. The information sent to the HLR is normally the SS7 address of the new VLR. 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.

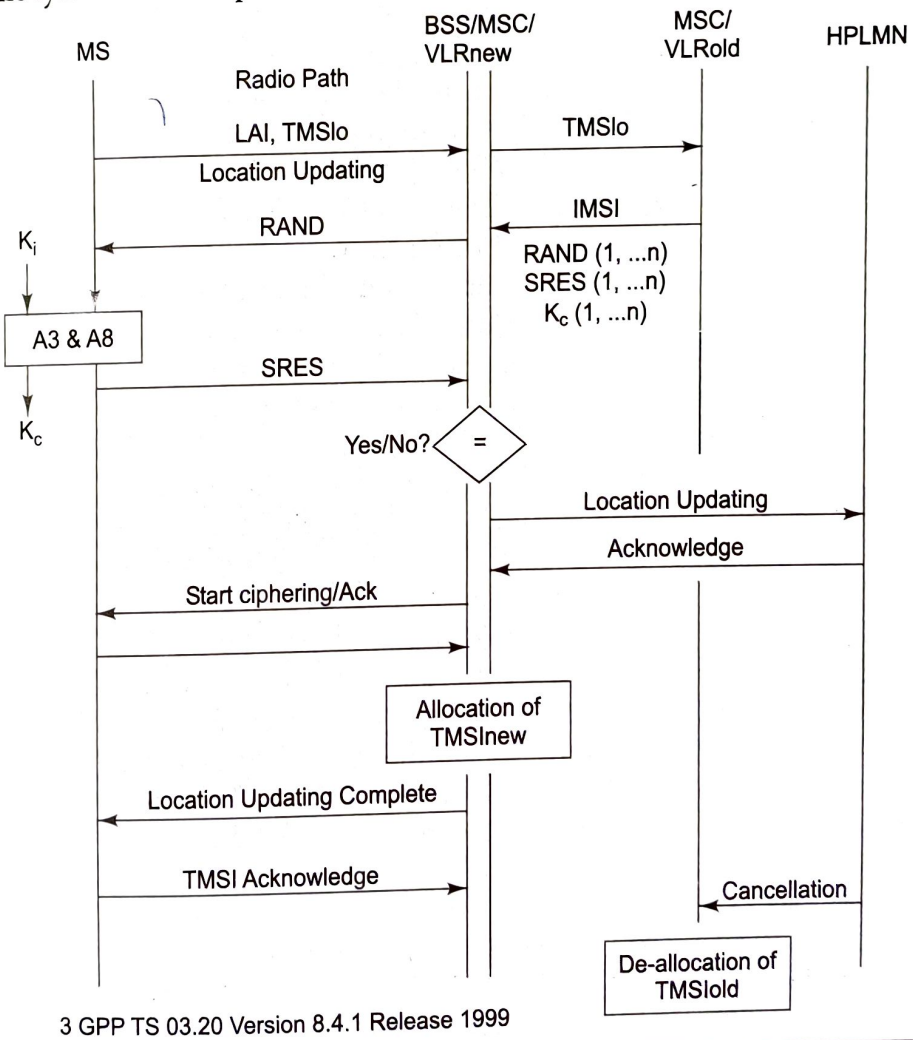
An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch, which is able to interrogate the subscriber's HLR to obtain routing information and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. Though the GMSC function is distinct from the MSC function, it is usually implemented within an MSC. The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also

procedure. The MSC in this case will terminate the procedure with the old BSS by sending a Clear_Command with cause "Handover successful". When the MS is successfully in communication with the network, i.e., the RR message Handover_Complete has been received from the MS, then the new BSS will immediately send a BSSMAP message Handover_Complete to the MSC and terminate the procedure. The MSC in this case will terminate the procedure with the old BSS by sending a Clear_Command with cause "Handover successful".

5.8.4 Authentication and Security Issues during Handover

GSM uses A3, A8, and A5 algorithms (see Section 5.10) for security. A3 algorithm is used to authenticate the subscriber; A8 algorithm is used to generate the ciphering key K_c; and, A5 algorithm is used to cipher everything that is transmitted over the air that include both signal and traffic. Security issues in GSM network are covered in detail in GSM standard 03.20.

When a handover occurs, the necessary information (e.g., key K_c, initialization data) is transmitted within the system infrastructure to enable the communication to proceed from the old BSS to the new BSS, and the synchronization procedure is resumed. The key K_c remains unchanged at handover.



3 GPP TS 03.20 Version 8.4.1 Release 1999

Figure 5.11 Normal Location Updating Procedure (Fig. 5.1)

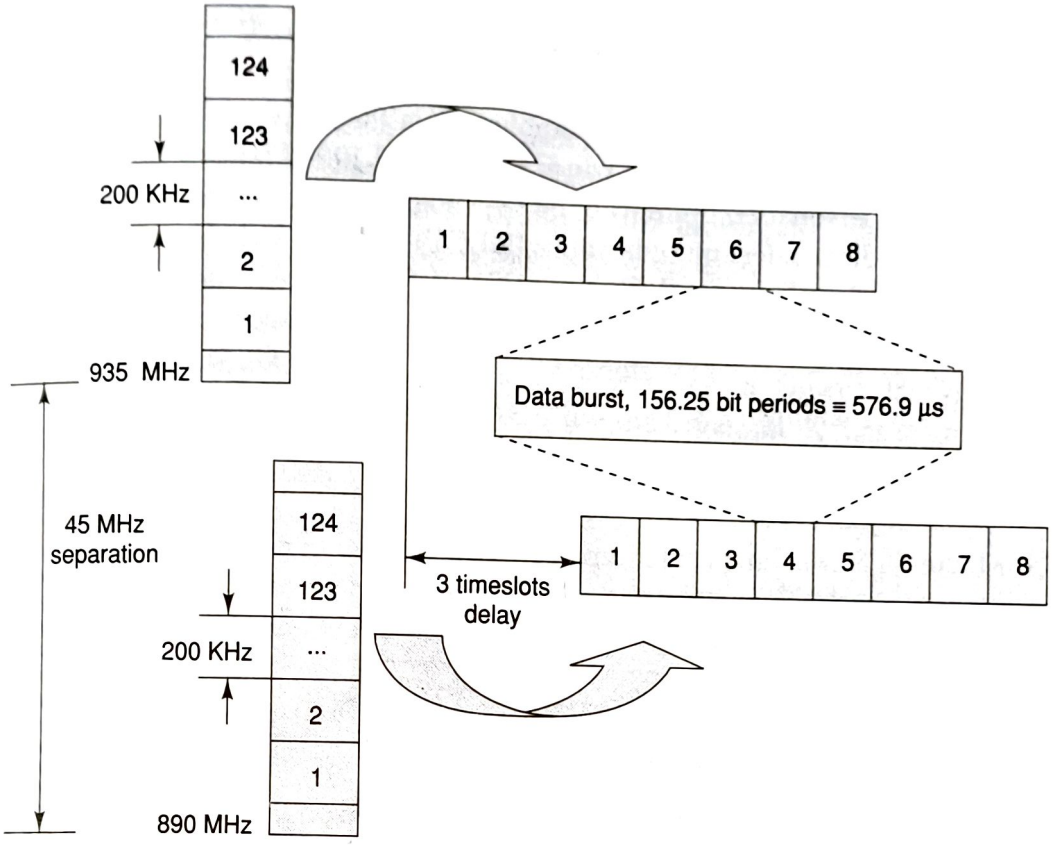


Figure 5.12 Carrier Frequencies and TDMA Frames

position of their corresponding burst periods. 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 (Fig. 5.13). Out of the 26 frames, 24 are used for traffic, one is used for the Slow Associated Control Channel (SACCH) and one is currently unused.

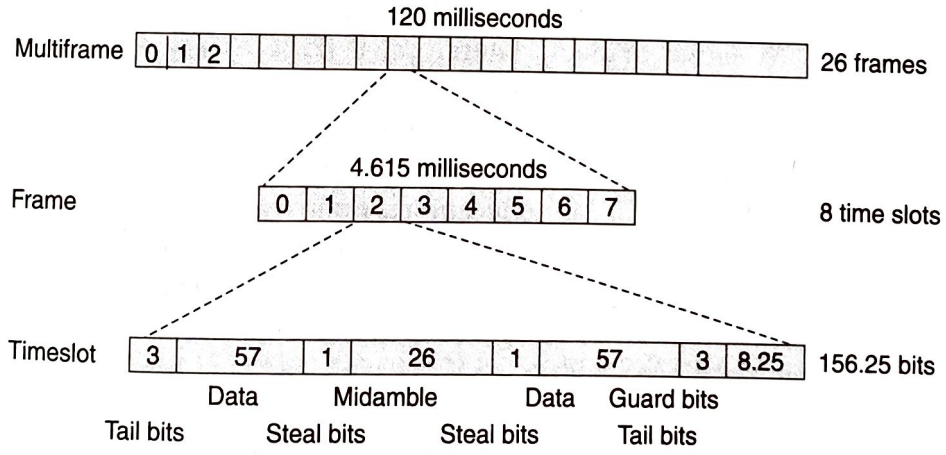


Figure 5.13 Organization of Bursts and TDMA Frames

CHAPTER 6

Short Message Service (SMS)

6.1 MOBILE COMPUTING OVER SMS

GSM supports data access over CSD (Circuit Switched Data). GSM is digitized but not packetized. In case of CSD, a circuit is established and the user is charged based on the time the circuit is active and not on the number of packets transacted. GPRS (General Packet Radio Service), also known as 2.5G, which is the next phase within the evolution of GSM, supports data over packets. WAP is a data service supported by GPRS and GSM to access Internet and remote data services. WAP has been covered in Chapter 8. Other data services in GSM include Group 3 facsimile, which is supported by use of an appropriate fax adaptor. A unique data service of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS enables sending and receiving text messages to, and from, GSM mobile phones. In this chapter we discuss SMS and developing applications using SMS bearer.

6.2 SHORT MESSAGE SERVICE (SMS)

Like many other eccentric technologies, SMS was also allegedly the right idea at the wrong time. On December 3, 1992, a scientist named Neil Papworth at Sema, a British technology company, sent the first text message "Merry Christmas" to the GSM operator Vodafone. It was sent to Vodafone director Richard Jarvis in a room at Vodafone's HQ in Newbury in southern England. The message was an overly premature seasonal greeting, some three weeks ahead of the festivities. Vodafone offered this service as a text messaging service with a brand name TeleNotes service targeted for the business community. The service was not at all popular in its early days. SMS was almost forgotten and became an unwanted child until seven years later in 1999 when other mobile phone operators started to allow customers to swap SMS. Today SMS is the most popular data bearer/service within GSM with an average of one billion SMS messages (at the end of 2002) transacted every day around the world, with a growth of on an average half a billion every month. The SS7

signaling channels are always physically present but mostly unused, be it during an active user connection or in the idle state. It is, therefore, quite an attractive proposition to use these channels for transmission of used data. SMS uses the free capacity of the signaling channel. Each short message is up to 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characters (some European alphabets) are used, and 70 characters in length when non-Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16 bit Unicode).

6.2.1 Strengths of SMS

Following is the list of unique characteristics of SMS, which make this an attractive bearer for mobile computing.

Omnibus nature of SMS: SMS uses SS7 signaling channel, which is available throughout the world. SMS is the only bearer that allows a subscriber to send a long distance SMS without having long distance subscription. For example, you cannot make a voice call to a mobile phone in UK unless you have an international calling facility. However, you can send a SMS to a subscriber in UK, without having an international call facility.

Stateless: SMS is sessionless and stateless. Every SMS message is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging. SMS can be used for proactive information dissemination for "unsolicited response" and business triggers generated by applications (referred as "Push" in Fig. 8.4).

Asynchronous: In HTTP, for every command (e.g., GET or POST) there is a request and a response pair making it synchronous at the transaction level. Unlike HTTP, SMS is completely asynchronous. In case of SMS, even if the recipient is out of service, the transmission will not be abandoned. Therefore, SMS can be used as message queues. In essence, SMS can be used as a transport bearer for both synchronous (transaction oriented) and asynchronous (message queue and notification) information exchange.

Self-configurable and last mile problem resistant: SMS is self-configurable. In case of Web or WAP, it is no trivial task to connect to a service from a foreign network without any change in the configuration or preference setting. The device needs to be configured interactively by the user or system administrator to access the network. This makes the access dependent on the last mile. SMS has no such constraints. While in a foreign network, one can access the SMS bearer without any change in the phone settings. The subscriber is always connected to the SMS bearer irrespective of the home and visiting network configurations. While roaming in a foreign network, even if the serving network does not have an SMSC (SMS Center) or SC (Service Center), SMS can be sent and received.

Non-repudiable: SMS message carries the SC and the source MSISDN as a part of the message header. Unlike an IP address it is not easy to handcraft an MSISDN address in the SMS. It is possible for an application connected to an SMS to handcraft an MSISDN address like "999" or even alphabetic addresses like "MYBANK". However, an application can not handcraft the SC address. Therefore, an SMS can prove beyond doubt the origin of itself.

Always connected: As SMS uses the SS7 signaling channel for its data traffic, the bearer media is always on. User cannot SWITCH OFF, BAR or DIVERT any SMS message. When a phone is busy and a voice, data or FAX call is in progress, SMS message is delivered to the MS (Mobile Station) without any interruption to the call.

6.2.2 SMS Architecture

SMS are basically of two types, SM MT (Short Message Mobile Terminated Point-to-Point), and SM MO (Short Message Mobile Originated Point-to-Point). SM MT is an incoming short message from the network side and is terminated in the MS. SM MO is an outgoing message, originated in the user device (MS), and forwarded to the network for delivery. For outgoing message, the path is from MS to SC via the VLR and the IWMSC function of the serving MSC, whereas for incoming message the path is from SC to the MS via HLR and the GMSC function of the home MSC (Fig. 6.1).

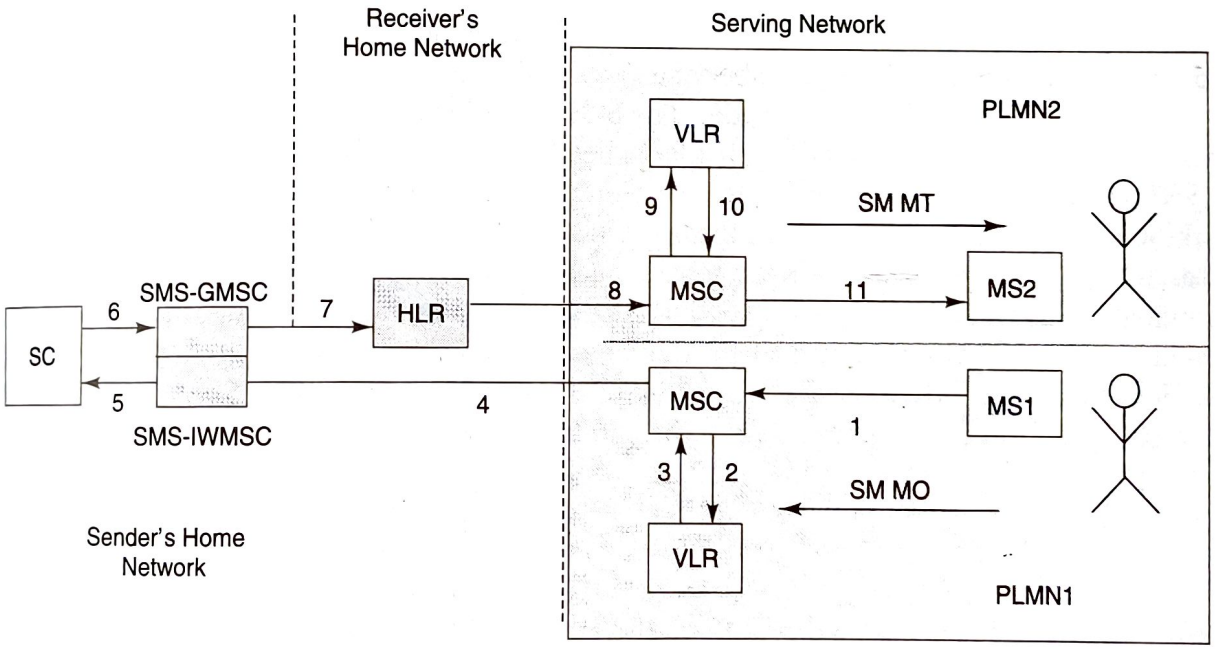


Figure 6.1 Flow of SMS between Two MS

To use SMS as a bearer for information exchange, the Origin server or the Enterprise server needs to be connected to the SC through a short message entity (SME) as in Figure 6.2. The SME in this case works as an SMS gateway, which interacts to the SC in one side, and the enterprise server on the other side.

6.2.3 Short Message Mobile Terminated (SM MT)

For an SM MT message, the message is sent from SC to the MS. This whole process is done in one transaction (Fig. 6.2). For the delivery of MT or incoming SMS messages, the SC of the serving

network is never used. This implies that an SMS message can be sent from any SC in any network to a GSM phone anywhere in the world. This makes any SM MT message mobile operator independent.

Figure 6.2 Interface Involved in the SM MT Procedure

6.2.4 Short Message Mobile Originated (SM MO)

SM MO is an outgoing message originated in the MS where generally the user types in a message and sends it to another MSISDN number or an application. For an MO message, the MSC forwards the message to the home SC of the sender. The SC is an independent computer in the network and works as a store and forward node with a large database. The database is used to store the SMSs. In SS7 terminology SC is an SCP (Service Control Point) within the SS7 cloud. MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as an MO message (Fig. 6.3). In the second phase, the message is sent from the home SC to the receiving MS as an MT message (Fig. 6.2). It is possible to attempt to send an SMS message to an invalid MSISDN number. In such a case, the message will be sent successfully from the MS to the SC. However, it will fail during the SC to the MS transfer. The user will see SM MO message sent successfully but SM MT message delivery would fail.

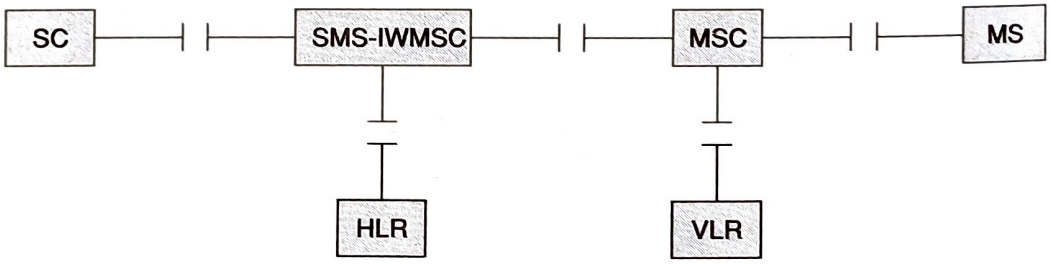


Figure 6.3 Interface Involved in the Short Message Mobile Originated (SM MO) Procedure

6.2.5 SMS as an Information Bearer

SMS is a very popular bearer in the person-to-person, mobile-to-mobile or point to point messaging domain. However, it is gaining popularity in other verticals like enterprise applications, services provided by independent service providers as ASP (Application Service Provider), and notification services, where one endpoint is a mobile phone but the other endpoint is a mobile application. Here SMS functions as an input-output media for information exchange for a mobile application (Fig. 6.4).