Wireless & Mobile Computing

UNIT IV

GSM REFERENCE ARCHITECTURE

GSM means Global System for mobile communication. GSM is generally utilized mobile correspondence framework on the planet. GSM framework was produced as an advanced framework utilizing time division multiple access (TDMA) method for correspondence reason. GSM otherwise called 2G network was produced at Bell Laboratories in 1970. It is generally utilized portable correspondence framework on the planet.

Global System for Mobile (GSM) is a second generation cellular system standard that was developed to solve the fragmentation problems of the first cellular systems in Europe. GSM is the world's first cellular system to specify digital modulation and network level architectures and services. Before GSM, European countries used different cellular standards throughout the continent, and it was not possible for a customer to use a single subscriber unit throughout Europe. GSM was originally developed to serve as the pan-European cellular service and promised a wide range of network services through the use of ISDN. GSM's success has exceeded the expectations of virtually everyone, and it is now the world's most popular standard for new cellular radio and personal communication equipment throughout the world. It is predicted that by the year 2000, there will be between 20 and 50 million GSM subscribers worldwide.

The task of specifying a common mobile communication system for Europe in the 900 MHz band was taken up by the GSM (Groupe spe'cial mobile) committee which was a working group of the Confe'rence Europe'ene Postes des et Telecommunication (CEPT). Recently, GSM has changed its name to the Global System for Mobile Communications for marketing reasons. The setting of standards for GSM is currently under the aegis of the European Technical Standards Institute (ETSI).

GSM was first introduced into the European market in 1991. By the end of 1993, several non European countries in South America, Asia, and Australia had adopted GSM and the technically equivalent offshoot, DCS 1800, which supports Personal Communication Services (PCS) in the 1.8 GHz to 2.0 GHz radio bands recently created by governments throughout the world.

GSM Services and Features

GSM services follow ISDN guidelines and are classified as either teleservices or data services. Teleservices include standard mobile telephony and mobile-originated or base originated traffic, Data services include computer-to computer communication and packet switched traffic. User services may be divided into three major categories:

• Telephone services, including emergency calling and facsimile. GSM also supports Videotex and Teletex, though they are not integral parts of the GSM standard.

• Bearer services or data services which are limited to layers 1, 2, and 3 of the open system interconnection (OSI) reference model. Supported services include packet switched protocols and data rates from 300 bps to 9.6 kbps. Data may be transmitted using either a transparent mode (where GSM provides standard channel coding for the user data) or non transparent mode (where GSM offers special coding efficiencies based on the particular data interface).

• Supplementary ISDN services, are digital in nature, and include call diversion, closed user groups, and caller identification, and are not available in analog mobile networks. Supplementary services also include the short messaging service (SMS) which allows GSM subscribers and base stations to transmit alphanumeric pages of limited length (160 7 bit ASCII characters) while simultaneously carrying normal voice traffic. SMS also provides cell broadcast, which allows GSM base stations to repetitively transmit ASCII messages with as many as fifteen 93-character strings in concatenated fashion. SMS may be used for safety and advisory applications, such as the broadcast of highway or weather information to all GSM subscribers within From the user's point of view, one of the most remarkable features of GSM is the Subscriber Identity Module (SIM), which is a memory device that stores information such as the subscriber's identification number, the networks and countries where the subscriber is entitled to service, privacy keys, and other user-specific information. A subscriber uses the SIM with a 4-digit personal ID number to activate service from any GSM phone. SIM's are available as smart (credit card sized cards that may be inserted into any GSM phone) or plugin modules, which are less convenient than the SIM cards but are nonetheless removable and portable. Without a SIM installed, all GSM mobiles are identical and nonoperational. It is the SIM that gives GSM subscriber units their identity. Subscribers may plug their SIM into any suitable terminal — such as a hotel phone, public phone, or any portable or mobile phone — and are then able to have all incoming GSM calls routed to that terminal and have all outgoing calls billed to their home phone, no matter where they are in the world.

A second remarkable feature of GSM is the on-the-air privacy which is provided by the system. Unlike analog FM cellular phone systems which can be readily monitored, it is virtually impossible to eavesdrop on a GSM radio transmission. The privacy is made possible by encrypting the digital bit stream sent by a GSM transmitter, according to a specific secret cryptographic key that is known only to the cellular carrier. This key changes with time for each user. Every carrier and GSM equipment manufacturer must sign the Memorandum of Understanding (MoU) before developing GSM equipment or deploying a GSM system. The MoU is an international agreement which allows the sharing of cryptographic algorithms and other proprietary information between countries and carriers.

GSM System Architecture

Concept

The GSM system architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces. The subsystems are the Base Station Subsystem (BSS), Network and Switching Subsystem (NSS), and the Operation Support Subsystem (OSS). The Mobile Station (MS) is also a subsystem, but is usually considered to be part of the BSS for architecture purposes. Equipment and services are designed within GSM to support one or more of these specific subsystems. The BSS, also known as the radio subsystem, provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). The BSS also manages the radio interface between the mobile stations and all other subsystems of GSM. Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the NSS via the MSCs. The NSS manages the switching functions of the system and allows the MSCs to communication operation and maintenance of GSM and allows system engineers to monitor, diagnose, and troubleshoot all aspects of the GSM system. This subsystem interacts with the other GSM subsystems, and is provided solely for the staff of the GSM operating company which provides service facilities for the network. Figure 2 shows the block diagram of the GSM system architecture. The Mobile Stations (MS) communicate with the Base Station Subsystem (BSS) over the radio air interface. The BSS consists of many BSCs which connect to a single MSC, and each BSC typically controls up to several hundred Base Transceiver Stations (BTSs). Some of the BTSs maybe co-located at the BSC, and others may be remotely distributed and physically connected to the BSC by microwave link or dedicated leased lines. Mobile handoffs (called handovers, or HO, in the GSM specification) between two BTSs under the control of the same BSC are handled by the BSC, and not the MSC. This greatly reduces the switching burden of the MSC.

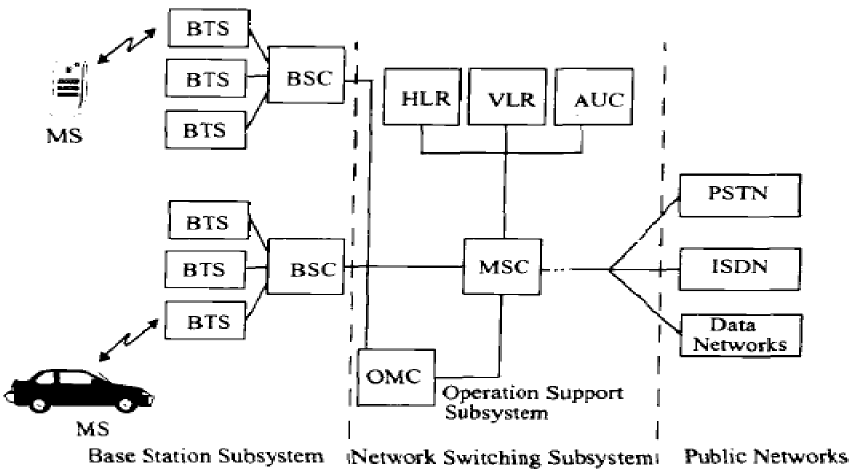


Fig2: GSM system Architecture

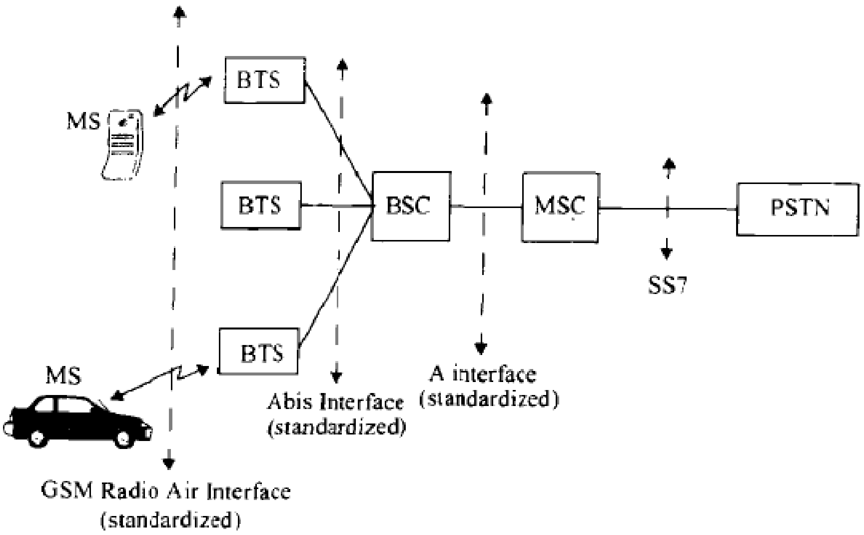


Fig 3 The various interfaces used in GSM

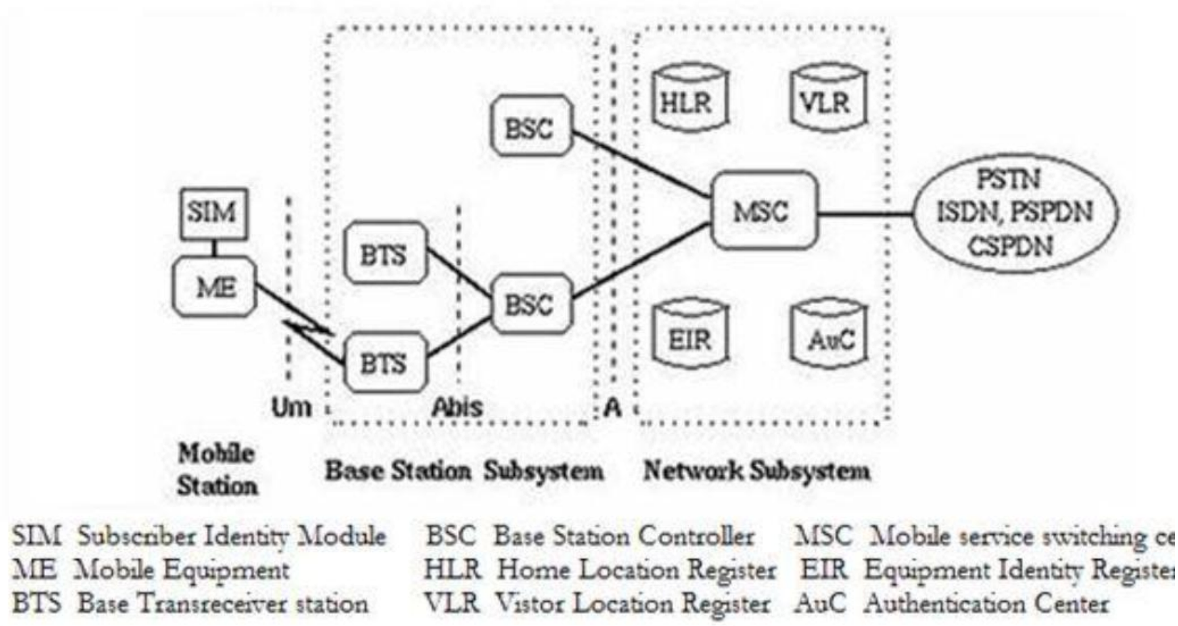
As shown in Figure 3, the interface which connects a BTS to a BSC is called the Abis interface. The Abis interface carries traffic and maintenance data, and is specified by GSM to be standardized for all manufacturers. In practice, however, the Abis for each GSM base station manufacturer has subtle differences, thereby forcing service providers to use the same manufacturer for the BTS and BSC equipment.

The BSCs are physically connected via dedicated leased lines or microwave link to the MSC. The interface between a BSC and a MSC is called the Air interface, which is standardized within GSM. The A interface uses an SS7 protocol called the Signaling Correction Control Part (SCCP) which supports communication between the MSC and the ESS, as well as network messages between the individual subscribers and the MSC. The A interface allows a service provider to use base stations and switching equipment made by different manufacturers.

The NSS handles the switching of GSM calls between external networks and the BSCs in the radio subsystem and is also responsible for managing and providing external access to several customer databases. The MSC is the central unit in the NSS and controls the traffic among all of the BSCs. In the NSS, there are three different databases called the Home Location Register (HLR), Visitor Location Register (VLR), and the Authentication Center (AUC). The HLR is a database which contains subscriber information and location information for each user who resides in the same city as the MSC. Each subscriber in a particular GSM market is assigned a unique International Mobile Subscriber Identity (IMSI), and this number is used to identify each home user. The VLR is a database which temporarily stores the IMSI and customer information for each roaming subscriber who is visiting the coverage area of a particular MSC. The VLR is linked between several adjoining MSCs in a particular market or geographic region and contains subscription information of every visiting user in the area. Once a roaming mobile is logged in the VLR, the MSC sends the necessary information to the visiting subscriber's FILE so that calls to the roaming mobile can be appropriately routed over the PSTN by the roaming user's HLR. The Authentication Center is a strongly protected database which handles the authentication and encryption keys for every single subscriber in the HLR and VLR. The Authentication Center contains a register called the Equipment Identity Register (EIR) which indentifies stolen or fraudulently altered phones that transmit identity data that does not match with information contained in either the HLR or VLR.

The OSS supports one or several Operation Maintenance Centers (OMC) which are used to monitor and maintain the performance of each MS, BS, BSC, and MSC within a GSM system. The OSS has three main functions, which are 1) to maintain all telecommunications hardware and network operations with a particular market, 2) manage all charging and billing procedures, and 3) manage all mobile equipment in the system. Within each GSM system, an OMC is dedicated to each of these tasks and has provisions for adjusting all base station parameters and billing procedures, as well as for providing system operators with the ability to determine the performance and integrity of each piece of subscriber equipment in the system

Components of Mobile Networks



The GSM network architecture consists of three major subsystems:

- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- The wireless link interface between the MS and the Base Transceiver Station (BTS), which is a part of BSS. Many BTSs are controlled by a Base Station Controller

(BSC). BSC is connected to the Mobile Switching Center (MSC), which is a part of NSS. Figure shows the key functional elements in the GSM network architecture.

1. Mobile Station (MS):

A mobile station communicates across the air interface with a base station transceiver in the same cell in which the mobile subscriber unit is located. The MS communicates the information with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS. The user’s voice information is interfaced with the MS through a microphone and speaker for the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements. The Mobile Equipment (ME) refers to the physical device, which comprises of transceiver, digital signal processors, and the antenna. The second element of the MS is the GSM is the Subscriber Identity Module (SIM). The SIM card is unique to the GSM system. It has a memory of 32 KB.

2. Base Station Subsystem (BSS):

A base station subsystem consists of a base station controller and one or more base transceiver station. Each Base Transceiver Station defines a single cell. A cell can have a radius of between 100m to 35km, depending on the environment. A Base Station Controller may be connected with a BTS. It may control multiple BTS units and hence multiple cells. There are two main architectural elements in the BSS – the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC). The interface that connects a BTS to a BSC is called the Abis interface. The interface between the BSC and the MSC is called the A interface, which is standardised within GSM.

3. Network and switching subsystem (NSS)

The NSS is responsible for the network operation. It provides the link between the cellular network and the Public switched telecommunicates Networks (PSTN or ISDN or Data Networks). The NSS controls handoffs between cells in different BSSs, authenticates user and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. In particular the switching subsystem consists of:

- Mobile switch center (MSC)
- Home location register (HLR)
- Visitor location Register (VLR)
- Authentications center (Auc)
- Equipment Identity Register (EIR)
- Interworking Functions (IWF)

The NSS has one hardware, Mobile switching center and four software database element: Home location register (HLR), Visitor location Register (VLR), Authentications center (Auc) and Equipment Identity Register (EIR). The MSC basically performs the switching function of the system by controlling calls to and from other telephone and data systems. It includes functions such as network interfacing and common channel signalling.

HLR: The HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber address, service type, current locations, forwarding address, authentication/ciphering keys, and billings information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscribes Identity (IMSI) number that is totally different from the ISDN telephone number. The HLR is the reference database that permanently stores data related to subscribers, including subscriber's service profile, location information, and activity status.

VLR: The VLR is temporary database software similar to the HLR identifying the mobile subscribers visiting inside the coverage area of an MSC. The VLR assigns a Temporary mobile subscriber Identity (TMSI) that is used to avoid using IMSI on the air. The visitor location register maintains information about mobile subscriber thatis currently physically in the range covered by the switching center. When a mobile subscriber roams from one LA (Local Area) to another, current location is automatically updated in the VLR. When a mobile station roams into anew MSC area, if the old and new LA's are under the control of two different VLRs, the VLR connected to the MSC will request data about the mobile stations from the HLR. The entry on the old VLR is deleted and an entry is created in the new VLR by copying the database from the HLR.

AuC: The AuC database holds different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user's identity and ensure the confidentiality of each call. The AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location register.

EIR: The EIR is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. This information is used to prevent calls from being misused, to prevent unauthorised or defective MSs, to report stolen mobile phones or check if the mobile phone is operating according to the specification of its type.

White list: This list contains the IMEI of the phones who are allowed to enter in the network.

Black list: This list on the contrary contains the IMEI of the phones who are not allowed to enter in the network, for example because they are stolen.

Grey list: This list contains the IMEI of the phones momentarily not allowed to enter in the the network, for example because the software version is too old or because they are in repair.

IWF-**Interworking Function:** It is a system in the PLMN that allows for non speech communication between the GSM and the other networks. The tasks of an IWF are particularly to adapt transmission parameters and protocol conversions. The physical manifestations of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network. The OSS (Operational Support Systems) supports operation and maintenance of the system and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network.

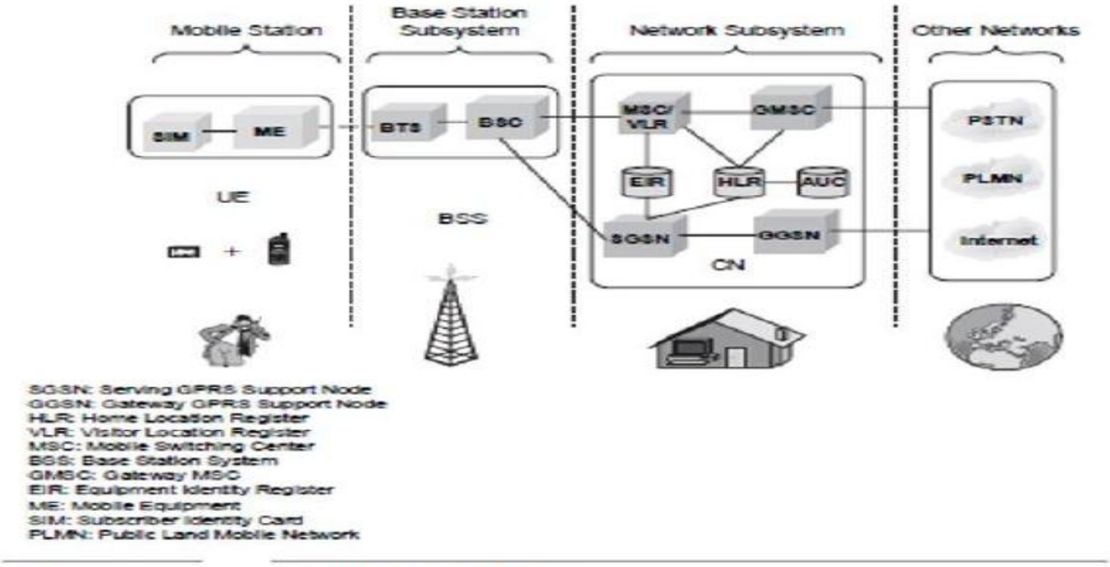


Figure architecture in GSM.

Fig above shows GSM architecture. The network manly consist of User Equipment (UE), Base transceiver station (BTS), Mobile switching center (MSC). The GSM contains most of the necessary capabilities to support packet transmission over GSM. The critical part in the GPRS network is the mobile to GSN (MS-SGSN) link which includes the MS-BTS, BTS-BSC, BSC-SGSN, and the SGSN-GGSN link the following Fig. shows block diagram of GSM architecture.

Base station(BSS)-- The following stations subsystem comprises of two parts:

1. Base Transceiver Station (BTS).
2. Base Station Controller(BSC). The BSS consists many BSC that connect to a single MSC. Each BSC controls upto several hundred BTS.

Base Transreciver Station(BTS)-BTS It has radio transreciever that define a cell and are capable of handling radio link protocols with MS. Functions of BTS are

1. Handelling radio link protocols
2. Providing FD communication to MS.
3. Interliving and deinterliving.

Base station controller(BSC) IT manages radio resources for one or more BTS. It controls several hundred BTS al are connected to single MSC. Functions of BTS are • To control BTS. • Radio resource management • Handoff management and control • Radio channel setup and frequency hoping.

User Equipment (UE)—These are the users .Number of users are controlled by one BTS. 1. The mobile stations (MS) communicate with the base station subsystem over the radio the radio interface.
2. The BSS called as radio the subsystem, provides and manages the radio transmission path between the mobile stations and the Mobile Switching Centre (MSC).It also manages radio interface between the mobile stations and other subsystems of GSM.
3. Each BSS comprises many Base Station Controllers (BSC) that connect the mobile station to the network and switching subsystem (NSS) through the mobile switching center.
4. The NSS controls the switching functions of the GSM system. It allows the mobile switching center to communicate with networks like PSTN, ISDN, CSPDN, PSPDN and other data networks.
5. The operation support system (OSS) allows the operation and maintenance of the GSM system. It allows the system engineers to diagnose, troubleshoot and observe the parameters of the GSM systems. The OSS subsystem interacts with the other subsystems and is provided for the GSM operating company staff that provides service facilities for the network.

Network subsystem(NSS) 1.It handles the switching of GSM calls between external networks and indoor BSC
2.It includes three different data bases for mobility management as
A .HLR (Home Location Register)
B .VLR (Visitor Location Register)
C. AUC (Authentication center)

Mobile switching center (MSC)-- It connects fix networks like ISDN ,PSTN etc. Following are the functions of MSC

1. Call setup, supervision and relies
2. Collection of billing information
3. Call handling / routing
4. Management of signalling protocol
5. Record of vlr and hlr

HLR (Home Location Register) - Call roaming and call routing capabilities of GSM are handled. It stores all the administrative information of sub scriber registered in the networks. It maintains unique international mobile subscriber identity.(IMSI).

The **home location register** (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. There can be several logical, and physical, HLRs per public land mobile network (PLMN), though one international mobile subscriber identity (IMSI)/MSISDN pair can be associated with only one logical HLR (which can span several physical nodes) at a time[1].

The HLRs store details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is the primary key to each HLR record.

Another important item of data associated with the SIM are the MSISDNs, which are the telephone numbers used by mobile phones to make and receive calls. The primary MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Each MSISDN is also a unique key to the HLR record. The HLR data is stored for as long as a subscriber remains with the mobile phone operator.

Examples of other data stored in the HLR against an IMSI record is:

- GSM services that the subscriber has requested or been given.
- General Packet Radio Service (GPRS) settings to allow the subscriber to access packet services.
- Current location of subscriber (VLR and serving GPRS support node/SGSN).
- Call divert settings applicable for each associated MSISDN.

The HLR is a system which directly receives and processes MAP transactions and messages from elements in the GSM network, for example, the location update messages received as mobile phones roam around.

Other GSM core network elements connected to the HLR

The HLR connects to the following elements:

- The G-MSC for handling incoming calls
- The VLR for handling requests from mobile phones to attach to the network
- The SMSC for handling incoming SMSs
- The voice mail system for delivering notifications to the mobile phone that a message is waiting
- The AuC for authentication and ciphering and exchange of data (triplets)

Procedures implemented

The main function of the HLR is to manage the fact that SIMs and phones move around a lot. The following procedures are implemented to deal with this:

- Manage the mobility of subscribers by means of updating their position in administrative areas called 'location areas', which are identified with a LAC. The action of a user of moving from one LA to another is followed by the HLR with a Location area update procedure.
- Send the subscriber data to a VLR or SGSN when a subscriber first roams there.
- Broker between the G-MSC or SMSC and the subscriber's current VLR in order to allow incoming calls or text messages to be delivered.
- Remove subscriber data from the previous VLR when a subscriber has roamed away from it.

VLR (Visitor Location Register) - It is a temporary data base. It stores the IMSC number and customer information for each roaming customer visiting specific MSC.

VLR is a database of the MSs (Mobile stations) that have roamed into the jurisdiction of the Mobile Switching Center (MSC) which it serves. Each main base station in the network is served by exactly one VLR (one BTS may be served by many MSCs in case of MSC in pool), hence a subscriber cannot be present in more than one VLR at a time.

The data stored in the VLR has either been received from the **Home Location Register (HLR)**, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface. Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it also updates the HLR of the mobile subscriber, appraising it of the new location of that MS. If VLR data is corrupted it can lead to serious issues with text messaging and call services.

Data stored include:

- IMSI (the subscriber's identity number).
- Authentication data.
- MSISDN (the subscriber's phone number).
- GSM services that the subscriber is allowed to access.
- access point (GPRS) subscribed.
- The HLR address of the subscriber.
- SCP Address(For Prepaid Subscriber).

Procedures implemented

The primary functions of the VLR are:

- To inform the HLR that a subscriber has arrived in the particular area covered by the VLR.
- To track where the subscriber is within the VLR area (location area) when no call is ongoing.
- To allow or disallow which services the subscriber may use.
- To allocate roaming numbers during the processing of incoming calls.
- To purge the subscriber record if a subscriber becomes inactive whilst in the area of a VLR. The VLR deletes the subscriber's data after a fixed time period of inactivity and informs the HLR (e.g., when the phone has been switched off and left off or when the subscriber has moved to an area with no coverage for a long time).
- To delete the subscriber record when a subscriber explicitly moves to another, as instructed by the HLR.

Operation subsystem(OSS) - It manages all mobile equipment in the system 1)management for charging and billing procedure 2)To maintain all hardware and network operations.

CALL ESTABLISHMENT IN GSM

Call establishment in POTS starts with a dialing process that transfers the number to the nearest PSTN switch where a routing algorithm finds the best connection through intermediate switches to the destination. After establishment of the link, the last switch (end office) at the destination sends a signal back to the source to announce whether the destination is available or busy that is signaled to the user at the source. When the destination POTS terminal is off-hook, another signal is sent to the source end-office to stop the waiting tone and establish the traffic line. In the mobile environment we have two separate call establishment procedures for mobile-to-fixed and fixed-to-mobile calls. Mobile-to-mobile calls are a combination of the two. The following two examples provide the detailed procedure in the GSM network for both types of call establishment.

Mobile Originated Call

The five-step procedure in POTS for call setup changes to a 15-step mobile originated call establishment procedure in the GSM. As shown in Figure 6 , the first five steps are similar to the registration process in GSM, except that these are done to prepare for call establishment. The next two steps start ciphering (encryption) to provide a protection against eavesdropping. The rest of the steps are similar to those in wired networks except that we have an additional traffic channel assignment procedure.

Steps	MS	BTS	BSC	MSC
1. Channel request	→	→		
2. Channel assigned	←	←		
3. Call establishment request	→	→	→	
4. Authentication request	←	←	←	
5. Authentication response	→	→	→	
6. Ciphering command	←	←	←	
7. Ciphering ready	→	→	→	
8. Send destination address	→	→	→	
9. Routing response	←	←	←	
10. Assign traffic channel	→	→		
11. Traffic channel established	←	←		
12. Available/busy signal	←			
13. Call accepted	←	←	←	
14. Connection established	→	→	→	
15. Information exchange	←→			

Fig 6 Mobile originated call

Mobile Terminated Call

The most complicated call establishment is for the situation where a fixed telephone dials a mobile visiting another MSC. As shown in Figure 7 , after dialing, the PSTN directs the call to the MSC identified by the destination address. The MSC requests routing information from the HLR. Because, in this case, the mobile is roaming in the area of a different MSC, the address of the new MSC is given to MSC, and it contacts the new MSC. At the destination MSC, the VLR initiates a paging procedure in all BSSs under the control of the MSC holding the registration. After a reply from the MS, the VLR sends the necessary parameters to the MSC to establish the link to the MS.

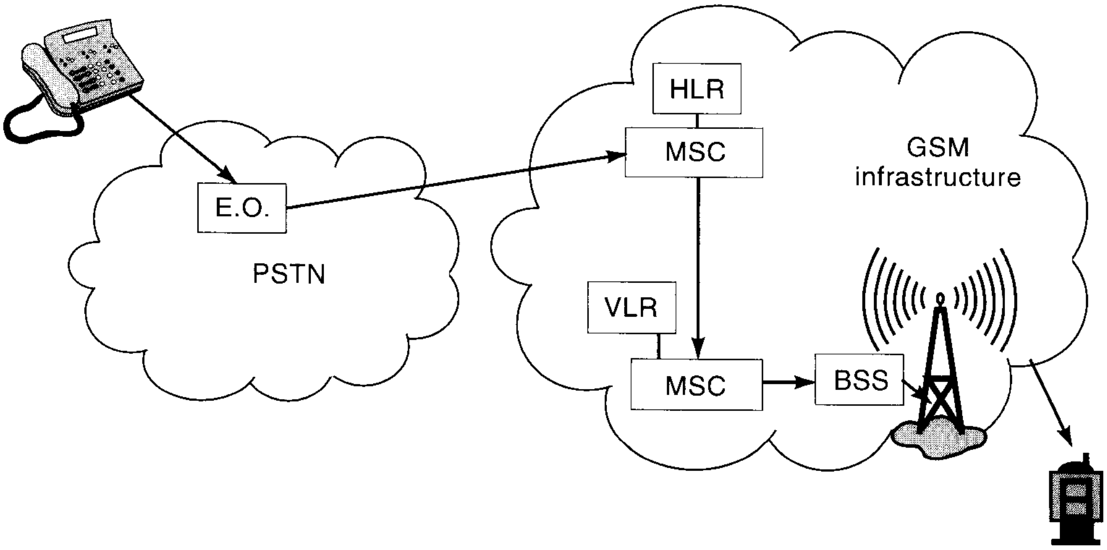


Fig7 Mobile terminated call in a visiting network

HAND-OFF SCENARIOS IN GSM

Four Mechanisms are embedded in all voice-oriented wireless networks which allow a mobile to establish and maintain a connection with the network. These mechanisms are registration, call establishment, handover(or handoff) and security. Registration takes place as soon as one turns the mobile unit on, call establishment occurs when the user initiates or receives a call, handover helps the MS to change its connection point to the network, and security protects the user from fraud and evesdropping.

The process of handover or handoff within any cellular system is of great importance.Cellular systems require handover procedures, as single cells do not cover the whole service area,but only up to at most about 25kms around each antenna. The smaller the cell size and the faster the movement of a mobile station through the cells(up to 250 km/h for GSM), the more handoffs of ongoing calls are required. However, a handoff should not cause a cut-off, i.e. “dropping a call in progress”. Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network. Accordingly GSM handover was an area to which particular attention was paid when developing the standard.

There are two basic reasons for a handoff (a.k.a handover in the E.U):

1. The mobile station moves out of range of a BTs or a particular antenna of the BTS. Thus, the received signal level becomes lower continuously until its falls underneath the minimum threshold required for reliable communication. Or, the error rate may grow due to interference, the distance to the BTS may be too high(max. 35kms)etc. All these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.
2. The wired infrastructure (MSC,BSC) may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load(if possible). Thus handoff may happen due to load balancing.

Types of GSM handover

Within the GSM system there are four types of handover that can be performed for GSM only systems:

- ***Intra-BTS handover:*** This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver, but changes the channel or slot.
- ***Inter-BTS Intra BSC handover:*** This form of GSM handover or GSM handoff occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.
- ***Inter-BSC handover:*** When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.
- ***Inter-MSC handover:*** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

GSM Handover Process

Although there are several forms of GSM handover as detailed above, as far as the mobile is concerned, they are effectively seen as very similar. There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.

In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight. As a result the RF section of the mobile could be idle for 6 slots out of the total eight. This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable. In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighbouring BTSs via the Broadcast Channel (BCCH).

The mobile scans these and reports back the quality of the link to the BTS. In this way the mobile assists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand Over (MAHO).

The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile. It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.

If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile. It informs the BTS and the mobile of the change. The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.

A key element of the GSM handover is timing and synchronisation. There are a number of possible scenarios that may occur dependent upon the level of synchronisation.

- ***Old and new BTSs synchronised:*** In this case the mobile is given details of the new physical channel in the neighbouring cell and handed directly over. The mobile may optionally transmit four access bursts. These are shorter than the standard bursts and thereby any effects of poor synchronisation do not cause overlap with other bursts. However in this instance where synchronisation is already good, these bursts are only used to provide a fine adjustment.
- ***Time offset between synchronised old and new BTS:*** In some instances there may be a time offset between the old and new BTS. In this case, the time offset is provided so that the mobile can make the adjustment. The GSM handover then takes place as a standard synchronised handover.
- ***Non-synchronised handover:*** When a non-synchronised cell handover takes place, the mobile transmits 64 access bursts on the new channel. This enables the base station to determine and adjust the timing for the mobile so that it can suitably access the new BTS. This enables the mobile to re-establish the connection through the new BTS with the correct timing.

Inter-system handover

With the evolution of standards and the migration of GSM to other 2G technologies including to 3G UMTS / WCDMA as well as HSPA and then LTE, there is the need to handover from one technology to another. Often the 2G GSM coverage will be better then the others and GSM is often used as the fallback. When handovers of this nature are required, it is considerably more complicated than a straightforward only GSM handover because they require two technically very different systems to handle the handover.

These handovers may be called intersystem handovers or inter-RAT handovers as the handover occurs between different radio access technologies.

The most common form of intersystem handover is between GSM and UMTS / WCDMA. Here there are two different types:

- ***UMTS / WCDMA to GSM handover:*** There are two further divisions of this category of handover:

  Blind handover: This form of handover occurs when the base station hands off the mobile by passing it the details of the new cell to the mobile without linking to it and setting the timing, etc of the mobile for the new cell. In this mode, the network selects what it believes to be the optimum GSM based station. The mobile first locates the broadcast channel of the new cell, gains timing synchronisation and then carries out non-synchronised intercell handover.

  Compressed mode handover***:*** using this form of handover the mobile uses the gaps I transmission that occur to analyse the reception of local GSM base stations using the neighbour list to select suitable candidate base stations. Having selected a suitable base station the handover takes place, again without any time synchronisation having occurred.

  Handover from GSM to UMTS / WCDMA: This form of handover is supported within GSM and a "neighbour list" was established to enable this occur easily. As the GSM / 2G network is normally more extensive than the 3G network, this type of handover does not normally occur when the mobile leaves a coverage area and must quickly find a new base station to maintain contact. The handover from GSM to UMTS occurs to provide an improvement in performance and can normally take place only when the conditions are right. The neighbour list will inform the mobile when this may happen.