5.1 Introduction

Groupe Spéciale Mobile (GSM) was established by an initiative from Conference of European Post and Telecommunication (CEPT). The group had several committees with representatives from all major European telecom operators and manufacturers. The aim of these committees was to replace incompatible analog system by a pan-European digital land-mobile telecommunication service targeting mobile users. The responsibilities of developing the standards now rests with European Telecommunication Standard Institute (ETSI). ETSI re-defined the abbreviation GSM as Global System for Mobile. The aim of the standardization was to study and to develop a set of common specifications for European wide public mobile telephone system with following criteria:

- Good speech quality.
- Efficient spectral usage.
- Low terminal and service cost.
- Mobile hand-held terminal support.
- International roaming support.
- ISDN capabilities.

The first GSM standard was released in 1990. The commercial GSM service began in 1991. By 1993, GSM technology has spread outside Europe and became de facto world standard for mobile telephone service. GSM allows terminal mobility via a Subscriber Identity Module (SIM) which carries a personal number issued to the mobile user. SIM contains many subscriber related information including a personal identity number (PIN), and PIN unblocking code as safe guards against un-authorized use. Undoubtedly, GSM is most widely deployed and the fastest growing cellular based mobile telephone technology in the world today. It is still undergoing a continuous process of evolution. High Speed Circuit Switched Data (HSCSD), Enhanced Data rates for GSM Evolution (EDGE) and General Packet Radio Service (GPRS) were added to GSM network to provide better features, new functionalities and increased data rates. GPRS standards were released in 1997 by ETSI. It eliminates the annoying requirement for repetitive dial-ups for establishing connections and provides throughput in excess of 40 Kbps. Advanced competing technology like UMTS has entered into the commercial market for providing even better data rates than GPRS. However, in reality UMTS is not radically different from GSM. It redefines base station technology, but requires GSM as base support technology. In this chapter our discussion is mainly centred around the base GSM technology. We take a look on GPRS and also examine how UMTS has been positioned up the ladder of mobile communication technology by re-jigging GSM.

5.2 GSM Architecture

GSM network was developed on the generic cellular architecture discussed in the previous chapter. It employs mainly three basic equipment and modules for implementing the functionalities of mobile telephone network on the basis of cellular architecture. These are:

- Mobile Station (MS) or subscriber's equipment and modules.
- Base Station Subsystem (BSS).
- Network Subsystem (NSS).

Figure 5.1 outlines GSM architecture. As indicated by the figure above, MS consist of a subscriber equipment or handset and a SIM card. The five main components of network subsystem (NSS) are: AuC, HLR, VLR, MSC and EIR. Base Station Subsystem (BSS) has two major components, namely, Base Station controller (BSC) and Base Station (BS). Let us now examine various subsystems of GSM architecture in some details.

5.2.1 Mobile Station

A subscriber's equipment and the associated module consist of a hand-held equipment known as a Mobile Station (MS) (also known as Mobile Handset (MH)) and a Subscriber Identity Module (SIM).

Mobile Handset: The equipment or the MH is essentially a transmitter and a receiver station with circuits responsible for

- Time and frequency synchronizations

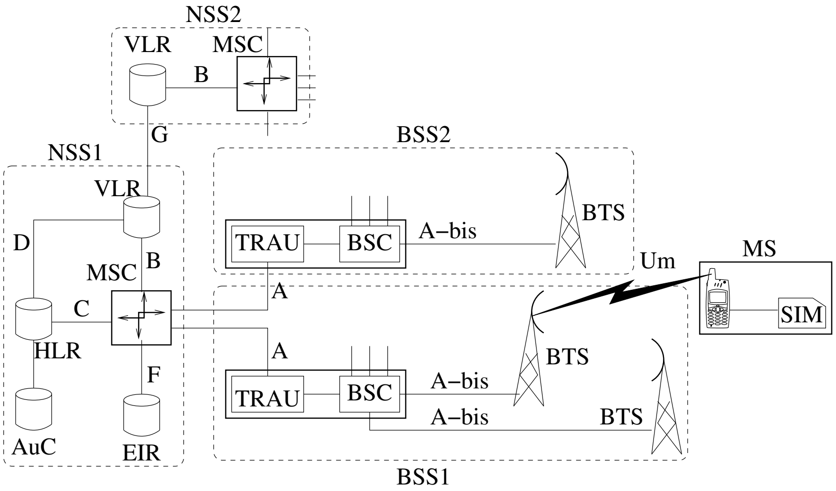


Figure 5.1: GSM architecture

- Measuring and reporting signal strengths from BSs
- Encoding speech and messages
- Coding to correct errors during transmission over air
- Compressing and decompressing data and speech.

Each mobile terminal has a unique identity known as International Mobile Equipment Identity (IMEI). IMEI number is usually inscribed on the battery compartment of an MS. This number can be retrieved from most mobile phones by keying ”*#06#”. An IMEI number maps a valid device to a user, and works as a safe-guard against stolen device. IMEI number is a 15 digit number which carries:

- A six digit Type Approval Code (TAC),
- A three digit Final Assembly Code (FAC),
- A six digit Serial Number (SN),
- A Spare digit (S).

On a user’s request the service provider can blacklist an IMEI, preventing unauthorized use of a stolen device. However, IMEI number have no relationship with the personal data concerning a user or a subscriber.

Subscriber Identity Module (SIM): A subscriber needs to insert a SIM into his/her mobile equipment to be able to make voice call or access data services. A SIM is a portable smart card having a small memory. It carries following important information related to a user:

1. International Mobile Subscriber's Identity (IMSI)
2. Authentication Key K_i
3. Cipher key K_c
4. Algorithms A3, A5 and A8

SIM also stores some permanent as well as temporary data related to user these include access control, location area identity, forbidden PLMN, additional GSM services and subscriber information.

IMSI and PIMSI (Packet IMSI) belong to the class of permanent data stored in a SIM. IMSI is a 64-bit field. It is sent to the GSM network when a user requests a connection. The network uses IMSI to retrieve information related to the subscriber's credentials and subscription. However, most of the time when MS is roaming TIMSI (a randomly generated data from IMSI) is sent in place of IMSI. TMSI is assigned by the locally responsible VLR. Therefore, it not possible to determine the presence of a mobile in a cell just by listening to radio channel.

The authentication key K_i is a 128-bit value also stored on database of GSM network known as Authentication Center (AuC). K_i can not be retrieved by SIM interface. SIM provides an algorithm to pass K_i to AuC. Algorithm A3 stored in SIM is used for forwarding key K_i for the purpose of authentication.

Algorithm $A5$ is used for encryption and decryption of data between MS and BS. For encryption SIM uses a cipher key K_c which is 64-bit value generated using a random number through algorithm $A8$.

5.2.2 Base Station Subsystem

The BSS consists of three components, Base Transceiver Station, Base Station Controller (BSC) and Transcoder and Rate Adaptation Unit (TRAU). A base transceiver station usually referred to as a Base Station (BS). It provides the last mile connectivity to a MS. Base station is the key communication equipment in a cell service area. It is responsible for communication with MS. Its functions include antenna, modem and signal processing.

Base Station Controller (BSC): It manages radio resources of one or more BSs. It handles channel setup, frequency hopping, handoffs and also acts as an interface between mobile switch center (MSC) and BSs. BSC receives measurements from MSs and controls handoffs for MSs from one BS to another. A BSC can manage upto 40 BSs. However, an MSC which controls several BSCs would typically provide a few lines to a BSC. Therefore, one of the important task of BSC is to act as a concentrator. Many low capacity BS connections to BSC are concentrated into a relatively small number of connections from an MSC.

Transcoding and Rate Adaptation Unit (TRAU): Mobile to mobile transmission path involves BSS to NSS and then NSS to BSS transitions. The bit rate supported by GSM radio interface is 13K bits for full rate and 5.6K bits for half rate. MSC is a PSTN/ISDN switch which supports data rate of 64K bits. The compression and formats of two sides are different which necessitates transcoding and rate conversion. Rate adaptation adapts the transmission rate of digital voice or data traffic on radio links (which is about 16Kbps) to the standard data rate of 64Kbps achievable from MSC through conventional networks. Transcoding involves conversion of formats as well a compression. The voice and data traffic originating from mobile stations through BSs are compressed and converted into 64 Kbps data format. The method consists of multiplexing a few of the low speed speech or data streams and convert them into standard 64 Kbps format. Using compression TRAU could bring reduction in the transmission cost by as much as 75%. TRAU is placed closer to MSC, between MSC and BSC. TRAU also generates comfort noise for discontinuous transmission (DTX). DTX is used to increase power efficiency in operation of transmitter. It takes advantage of the fact that in a normal conversation, only about 40% of an active connection time is used. The transmitter can be turned off during the silence period for power efficiency. The biggest challenge here is the detection of voice activity. The detection process must distinguish between noise and voice. If voice is misinterpreted as noise and transmitter is turned off annoying clipping will be heard at receiver end. On the other hand, if noise is misinterpreted as voice then efficiency of DTX goes down. So, TRAU generates comfort noise, matching the background noise, which indicates the receiver end that the transmitter is not dead.

5.2.3 Network Subsystem

Network subsystem is popularly known as switching subsystem. MSC is the key component of a GSM network subsystem. It provides the functionalities needed to handle mobile subscriber's handset such as registration, authentication, location updates, handoffs, connection routing, and mobility. It needs to keep track of updated status and location of a MS. The location database is partitioned into Home Location Register (HLR) and Visitors Location Register (VLR). Location databases may be stored in separate location servers, but VLR is usually co-located with MSC. The other elements of GSM network include:

1. Gateway MSC (GMSC), which is connected to PSTN and ISDN network,

2. Equipment Identity Registers (EIR), and

3. AUthentication Center (AUC).

EIR store MS's IMEI while AUthentication Center (AUC) is an important database used to authenticate the mobile user.

Guaranteeing transmission of voice or data of a given quality over the radio link is an important function of GSM network. There is another set of equally important functions which a GSM network should perform. Supporting user's mobility is one of these. The network should be able to detect movements of individual mobile users and switch any active connections to the channels under new cells to which the respective users may have migrated. The task of preserving an active connection is realized by implementing handoff (also known as handover) mechanism on GSM network. Handoff ensures that existing communication remains active across many transient movements of the users. The other important function of GSM network is to facilitate both national and international roaming support for the mobile subscribers. Allowing migration from one administrative network domain to another involve credential checks like identity, and authenticity. After that establishing user's credentials the network should be able to reroute connection and keep track of each user's locations as the user moves. The

GSM network provides a number of functions for efficient handling of roaming. These functions are handled through signaling protocols between the different components of the GSM networks mentioned above.

5.2.4 GSM Radio Resources

Before, discussing GSM protocols it is important to understand the radio resources and management of these resources. GSM uses a mix of FDMA and TDMA and combines this with frequency hopping for allocating radio resources. FDMA allocates a frequency to each user for the duration of his/her use. So for a FDMA system, a large frequency bands is needed to handle communication among large number of users. Since, only a limited radio frequency band is available, FDMA system is not scalable. TDMA allows several users to share a channel by time-sharing the usage. TDMA is normally used in conjunction with FDMA. A frequency channel is partitioned into fixed number of time-slots, and a selected time-slot is allocated to a user for the duration of his/her communication.

5.2.5 Channel types

The operating bands in GSM are 900 MHz, 1800 MHz and 1900 MHz. Each of the above frequency band is divided into uplink and downlink. For example, GSM 900 MHz split into: (i) 890-915MHz for uplink (mobile to BS), and (ii) 935-960MHz for downlink (BS to mobile). Each of these 25 MHz bands is partitioned into 124 of carriers of 200 KHz each leaving 200 KHz guard band from the left band edge. Similarly, the uplink and downlink bands for other two GSM operating bands are:

- 1800 MHz: 1710-1785 MHz for uplink, and 1805-1880 MHz downlink,
- 1900 MHz: 1850-1910 MHz for uplink, 1930-1990 MHz for downlink.

The 1800 MHz band provides 374 pair of carriers whereas the 1900 MHz band provides 299 pairs of carriers.

Each carrier is segmented using TDMA into 8 time-slots of duration 0.577 ms per-slot. So, each carrier lasts for 8 slots 0-7 called a frame or a burst. A frame/burst time is 0.577 ms×8 = 4.165 ms. The recurrent pattern of a particular time slot in each frame constitutes a single logical

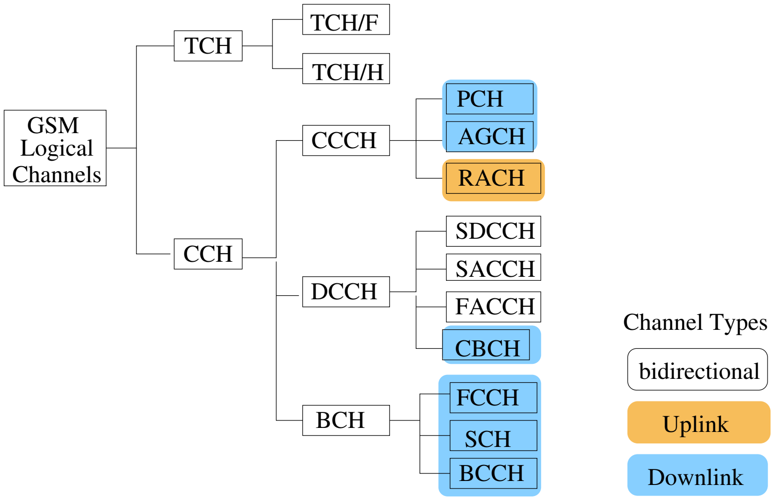


Figure 5.2: GSM channel classes.

channel. Notice that the repetition of one particular time slot occurs every 4.615 ms which is the time interval for one frame.

GSM logical channels are built on the top of physical channels. Logical channels address the issues related to information exchanges betwee MS and BSS. As Figure 5.2 indicates, GSM distinguishes between traffic channels (reserved for user data) and control channel (reserved for network control messages). Some of the channels are unidirectional while others are bidirectional. The unidirectional downlink channels are for communication from BS to MS. Same TDMA structuring of channels is used for both down and up links. However, the numbering of the slots for Traffic CHannels (TCH) is staggered by 3 time slots to prevent a mobile from transmitting and receiving at the same time. Traffic channels are defined using multiframe structures consisting of 26 TDMA frames with a recurrent interval of 120 ms (=4.615 ms×26). Out of 26 TDMA frames 24 are used for traffice, 1 frame is used for Slow Associated Channel and 1 frame is unused. Control channels are defined in a multiframe structure consisting of 51 TDMA frames having recurrent interval of 235.4 ms.

GSM control or signaling channels are divided into four classes, namely,

1. Broadcast CHannels (BCH),
2. Common Control CHannels (CCCH),

3. Dedicated Control CHannels (DCCH), and

4. Associate Control CHannels (ACCH).

The broadcast control channels are used by BS to provide synchronization information to MS. Depending on information flow, we can distinguish three different broadcast channels, viz., (i) Broadcast Control CHannel (BCCH), (ii) Synchronization CHannel (SCH) and (iii) Frequency Correction CHannel (FCCH). BS provides network parameters to MS over BCCH. SCH is used to provide training symbol sequence for demodulating transmitted information by BS. FCCH is reserved for providing frequency reference of the system for synchronization of MS.

The common control channels support establishing links between mobile stations and network. The important CCCH are: (i) Random Access CHannel (RACH), (ii) Access Grant CHannel (AGCH), (iii) Paging CHannel (PCH) and (iv) Notification CHannel (NCH). RACH is a purely uplink channel used by the mobiles to access of services such as voice call, SMS, responding to paging and sending registration. It is accessed in a competitive multiple access mode using the principles of slotted ALOHA. The remaining three control channels are downlink channels. PCH is used for searching or paging a mobile device by its IMSI or TMSI. AGCH is used to grant accesses when a mobile has either been successfully paged on PCH or it has initiated a request throgh RACH. It sets up signaling by assigning a stand-alone dedicated control channel (SDCCH) or a TCH to a mobile station. NCH is used to notify a group of mobiles about voice broadcast service. CCCH channels occupy slot 0 in a frame and repeat back every 51 frame times. When more capacity is required slots 2, 4, or 6 can be used.

Dedicated Control CHannels (DCCH) are for bidirectional information flow between mobile stations and base stations. Two main of DCCH are: (i) Stand-alone Dedicated Control CHannel (SDCCH), and (ii) Slow Associated Control CHannel (SACCH). A SDCCH channel is maintained between a mobile station (MS) and a BS for exchange of message relating to call establishment, authentication, location update, SMS, etc. Slow Associated Control CHannel (SACCH) is alway associated with a TCH or SDCCH. It is used to inform MS about frequencies of neighboring cells, time synchronization and power control on downlink. The uplink is used for sending signal measurements and other parameters from MS that aids in arriving at handover decisions. It can be used to transmit SMS if the associated with a

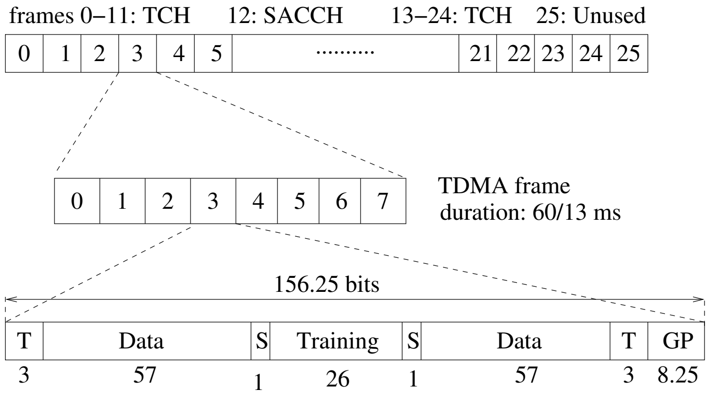


Figure 5.3: Structure of a normal GSM frame or burst.

TCH. This is the reason why an SMS can be delivered when the user is busy with a call.

A Fast Associated Control CHannel (FACCH) is not a control channel in true sense. It is a TCH that turns momentarily into a control channel thereby stealing some time slots from associated TCH. After the use of FACCH is over the channel turns back into the traffic channel. FACCH is used for call signaling including call disconnect, handover as well as call setup.

5.2.6 Frame structure

There are four types frame or burst structures, namely,

1. Normal frame, used to carry voice or data,

2. Frequency correction frame, used on FCCH,

3. Synchronization frame, used on SCH,

4. Random access, used in RACH.

Each of these frames has a length of 156.25 bits and duration 0.577 ms, but different structures. The first three frames carry 142 bits of information, while the information contents in the last frame is 77 bits. The structure of a normal frame is shown in Figure 5.3. The tail bits form a group 3 bits placed at the beginning and end of a frame to provide for ramping mobile's

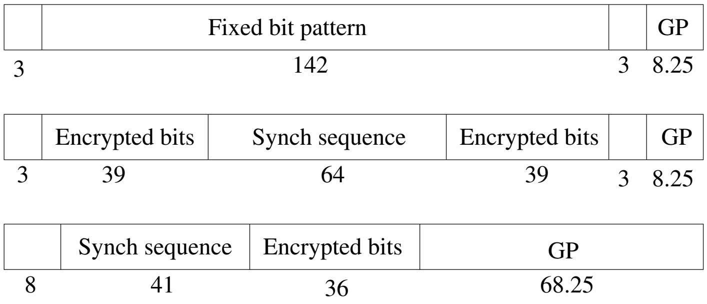


Figure 5.4: Structure of a normal GSM frame or burst.

power up or down. The data bits are coded in two groups of 57 bits each separated by 26 bits of training sequence. The training sequence is used for synchronization of the receiver to eliminate or mask multipath propagation effects. A guard period equivalent to 8.25 bits length is used avoid possible overlap of two mobiles during power build up time. There is 1 bit representing stealing flag after each group of Data bits. Stealing bit indicates whether the Data bits pertains to signal or user data. The Channel quality depends on propagation effects or multipath fading. To ensure average channel quality, a slow frequency hopping is employed. It changes frequency every frame time. Frequency hopping also reduces co-channel interference. The structure of the remaining three frames are shown in Figure 5.4.

Traffic channel frames are transmitted in groups of 26 known as *26-multiframe*. Since, transmit time of each frame is 4.615 ms, the transmit time for a 26-multiframe is 4.615 ms× 26 = 120 ms. Control frames, on the other hand, are transmitted in groups of 51 known as *51-multiframe*. A superframe consists of either 51 of 26-multiframes or 26 of 51-multiframes. A hiperframe consists of 2048 superframes. Thus, a hiperframe consists of 2048×26×51 frames, and has a transmit time 1566 ms.

5.3 GSM Signaling Protocols

The GSM has two different types of interfaces: `Um` and `Abis`. `Um` refers to air interface, and used for communicating between MS and BSS. `Abis` consists of 9 interfaces represented by `A` to `I`. The interface `A` is between BSS and MSC. It manages allocation of radio resources for mobility of MS and its

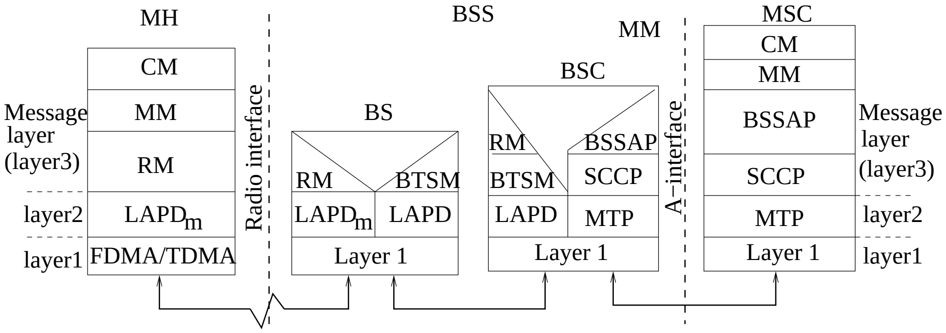


Figure 5.5: GSM network components.

management. The interfaces B to H are internal to MSC functions. Location database may be maintained at some location servers different from MSC. So, the wired interfaces B, C, D are for accessing HLRs and VLRs. Most MSCs store VLR database locally. So interface B is internal to MSC. C interface is between HLR and Gateway MSC (GMSC). The calls originating from outside GSM go through a GMSC to extract routing information. MAP/C protocol is used over C interface to get this information. MSC may also use this interface to forward billing information to HLR after connection has been setup. The D interface is between VLR and HLR. The data related to location of MS is exchanged over D interface using Mobile Application Part (MAP/D) protocol. The E interface is between two different MSCs. Handoff uses MAP/E protocol for exchange data related to handoff between anchor and relay MSCs. The F interface is between MSC and equipment identity register (EIR). It uses MAP/E protocol to check identity (IMEI) of MS. The G interface is between MSC and SMS gateway, it uses MAP/G protocol for transfer of short messages. The I is the interface between MS and MSC which relays transparently through BSS.

The signaling protocol of GSM consists of 3 layers. Figure 5.5 shows the structure of GSM protocol spread across the 4 GSM network entities, namely, MS, BS, BSC and MSC. Layer 1 and 2 respectively represent physical and data link layer. Layer 3 does not exactly represent the network layer as in OSI model. It is more appropriate to refer to layer 3 as message layer. This layer is used for communication of network resources, mobility, code format and all call related control messages between network entities.

Layer 2 protocol is provided by LAPD$_m$ which is a modified version of

LAPD (link access protocol for ISDN D-channel) of ISDN stack to work within the constraints of radio paths. The main modifications are for two reasons, namely,

1. Handling the requirements for tight synchronization of TDMA.
2. Eliminating redundant LAPD functions for bit error protection mechanism required over radio interface. In GSM it is handled in layer 1. LAPD flags are replaced by length indicator and FEC field is removed.

Layer 3 is consists of three sublayers, viz.,

1. Resouce management (RM) implemented over the link between MS and BSS, This sublayer oversees the establishment and the maintenance of stable uninterrupted communication links spanning both radio and wired links between MS and MSC. A part of RM's responsibility is also to manage handoffs. MS and BSS control most of the functions in RM, though some are also performed by MSC.
2. Mobility management (MM) sublayer handles mobility management and maintains the location information of MS apart from performing authentication and the related crypto controlled procedures.
3. Connection management (CM) sublayer sets up connection at user's request. Its functions are divided among three distinct tasks, viz., connection control, SMS and supplementary services. Connection control is related to circuit oriented services. SMS provides for point to point short message service. Supplementary services allows modification and checking of supplementary services.

Layer 3 also implements message transport part (MTP), and the signaling connection control part over the link between MSC and BSS. MM and CM sublayers provide certain functionalities of transport, session and presentation layers of OSI model.

5.4 Call setup

In GSM there is a distinction between the calls originating from a mobile and the calls terminating at a mobile. The first type of call is an outgoing call while the second one is an incoming call. In case of an incoming call the

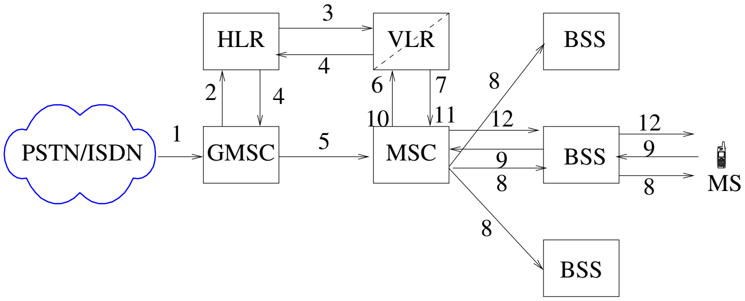


Figure 5.6: Protocol for incoming call to a mobile.

process will be same irrespective of the fact whether the call originates from a mobile or a PSTN landline. So, we examine the issues of call terminating at mobile separately from call originating at mobile.

5.4.1 Mobile terminated calls

An incoming call to a mobile is known as a Mobile Terminated Call (MTC). An incoming call is initiated when a subscriber dials a mobile ISDN number. Though mobile stations MS keep GSM network informed about their locations, it is not sufficient for setting up a call to a mobile station. After a calling party dials the number, PSTN first identifies the network to which the called MS belongs, and locates the GMSC for that network. Figure 5.6 illustrates the steps involved in processing of a MTC incoming call. As indicated by the figure, the process of call setup can be broken down into three basic tasks, namely, (i) finding route to the MSC responsible for the MS, (ii) paging the correct mobile and obtaining response from it, (iii) assigning a traffic channel for the call. Step 1-4 are for discovering the route to correct MSC, while the actual routing of call to the target MSC is done in step 5. Steps 6-8 are responsible for paging related task. Authentication, and security related checks are performed in steps 9-12. We provide a stepwise description of these activities below.

Step 1: The identity of network is extracted from MSISDN itself. PSTN sends initial address message (IAM) to the GMSC.

Step 2: GMSC forwards the MSISDN to HLR and requests for the routing information.

Step 3: HLR extracts the IMSI and SS7 address for the MSC/VLR which is currently servicing the MS. It then contacts the concerned MSC/VLR and requests it to assign an MSRN to the call. MSRN or mobile station roaming number is allocated by MSC/VLR from a set of available roaming numbers.

Step 4: MSC/VLR forwards the MSRN to HLR. HLR forwards both MSRN and routing information to GMSC. MSRN is used by GMSC for routing telephone call to target MSC.

Step 5: GMSC then send an IAM with MSRN to the servicing MSC/VLR for routing the call.

Step 6-7: After MSC/VLR receives the MSRN it releases the same so that MSRN now becomes available for reuse, and proceeds with call set up related activities. It gets LAI from VLR.

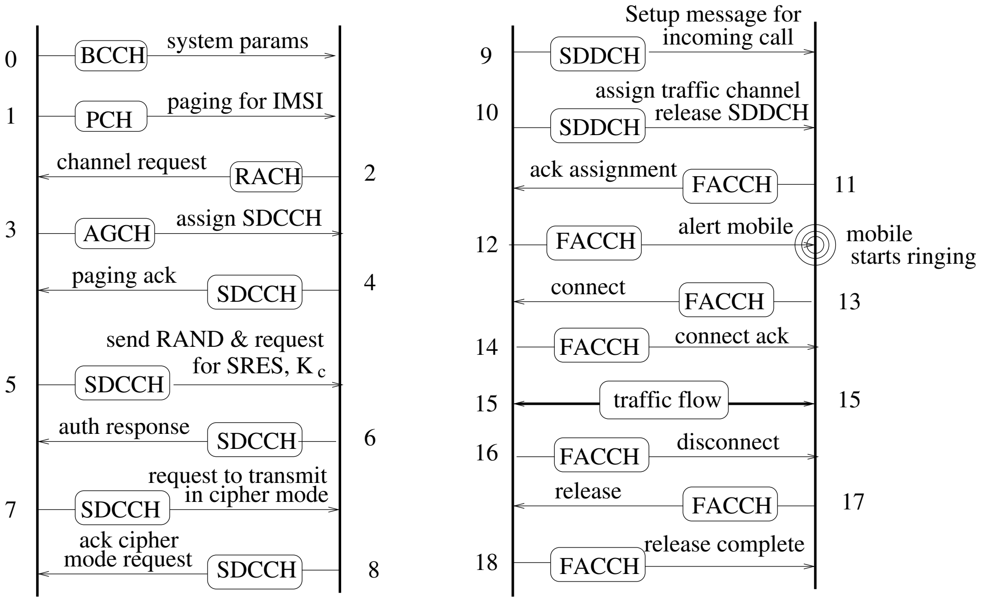
Step 8: MSC sends a paging request for locating the BS under which the called MS belongs.

Step 9: Since IMSI and TIMSI are included in the paging message, the called MS recognizes that the paging request is meant for it and responds.

Step 10-12: After getting paging response, the next task that network does is to establish the authenticity of the MS. Once authenticity check becomes successful, the mobile is requested to turn into cipher mode. Then the setup message for incoming call is also sent by the base station.

Finally, call is completes when caller disconnects. The process discussed gives a top level description of call setup procedure. It does not deal with the critical issues related to management of radio resources during call setup. Let us, therefore, examine how radio resources are allocated for establishing a successful call.

Initially the called mobile is in idle state. During this state a mobile handset keeps getting system parameters over broadcast control channel BCCH (step 0). As explained earlier, GMSC first obtains MSRN and contacts MSC for paging the called mobile on PCH channel (step 1). The mobile responds to the paging message over the uplink channel RACH (step 2) with intention to connect but does not respond to paging until it gets SDDCH assigned to



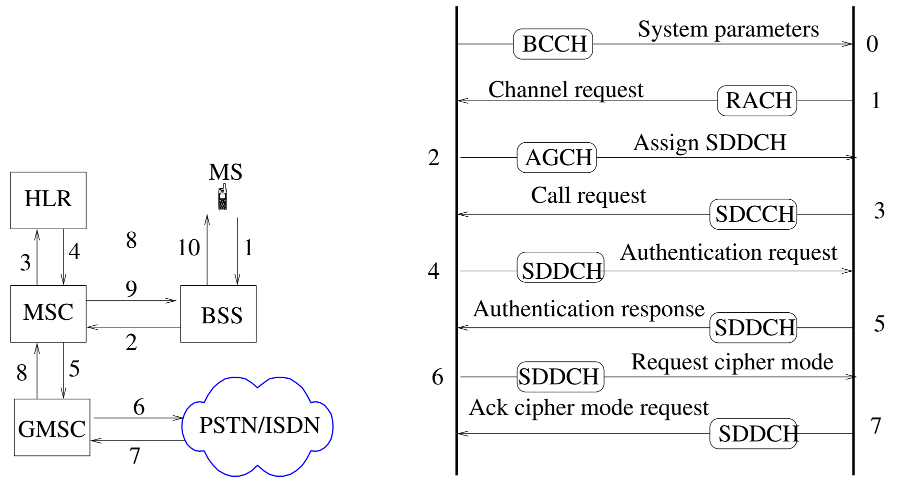
(a) Paging

(b) Call setup

Figure 5.7: Message flow over radio channels for mobile terminated call setup.

it. The message flow and over different radio channels for successful materialization of paging and subsequent authentication of mobile are shown in Figure 5.7(a). BSS responds to request of mobile's request for call setup on AGCH (step 3) by sending an immediate assignment message informing MS about the SDDCH. The network does yet not know the identity of the paged MS, until it sends a paging response over SDCCH (step 4). BSS then sends a random number for MS to generate cipher key and also sends challenge to MS (step 5) for the purpose of authentication. MS responds to this message by sending signaling response and generation the cipher key K_c (step 6). In the next step (step 7), BSS requests MS to transmit in cipher mode to which MS respond by an acknowledgement (step 8). All the message exchanges until this point (steps 3-8) takes place over SDDCH.

After mobile turns into cipher mode, BSS sends the setup message for incoming call and provides a traffic channel. The traffic channel is initially treated as control channel and once connection is fully established it turns into a traffic channel. So, BSS allocates traffic channel when it alerts the mobile about incoming call. In response to alert receiver generate ringing



(a) Signalling

(b) Radio interface

Figure 5.8: Signaling for mobile orignated call setup.

sound on the mobile. The channel activities for the call setup are illustrated in Figure 5.7(b).

5.4.2 Mobile originated calls

A mobile originated call may terminate at a mobile or a PSTN number. The signaling requirements for mobile orginated call is shown in Figure 5.8(a).

When a call request is made from a mobile device, network first seeks authenticity of subscriber (steps 1-2 in Figure 5.8(a). Once authenticity has been established, security checks are performed (steps 3-4). Check on resource availability (steps 5-8) is performed after security checks becomes successful. Finally the call is established (steps 9-10).

Earlier in previous section, we saw that availability radio resources is critical for a connection to materialize in mobile terminated call. Likewise, a call originating from mobile will required radio interface before establishment of a connection. A mobile originated call may terminated at mobile or a landline. We have already examined the channel activity at radio interface for a mobile terminated call. So, it suffices to just focus on the exchanges that occur on the radio channels at the caller's side.

Initially, when a mobile wishes to make a call, it sends a request on

RACH channel for the allocation of a stand-alone dedicated control channel (SDCCH). BSS uses AGCH to inform mobile about the access grant by allocating a SDCCH. Following the allocation of a SDDCH, the information relating to mobile's authentication and security checks are carried out. After this a traffic channel (TCH) is assigned to MS, and voice transfer occurs. illustrates the details of signaling mechanism for acquiring SDCCH and connecting a call. The channel activity which occur on radio interface at caller's side is illustrated in Figure 5.8(b).

5.4.3 Mobility Management

Mobility management is the key issue in GSM network. The issue of mobility management for an active connect with respect to generic cellular network earlier. In GSM implementation, a group of cells constitutes what is known as *paging area*. A group of cells defines a paging area. The whole service area is partitioned into a number of paging areas. For the purpose of establishing a call to a mobile, its paging area should be searched. If the mobile is active then it responds to paging message. However, it can do so only if the message is correctly directed to the mobile's paging area. Furthermore, paging area should not be very large. Otherwise, paging will generate unnecessary message flows over the network. To handle this problem, each mobile updates its location area identity (LAI) every time there is change in paging area. MS gets notification about LAI from base station. SIM stores current LAI and TMSI whenever a change occurs. If the LAI stored in SIM is not the same as the LAI being broadcast by BS, then a change is noted and the LAI update is performed by MS. MS needs radio resources to register the change in HLR. The channel activities for the same is explained in Figure 5.9.

Location update handles mobility when a mobile moves from one paging area to another. However, a more challenging problem in handling mobility occurs when a mobile is holding an active connection. In this case, the major requirement is requirement for channel switching. We have discussed mobility management of active mobile in cellular network in the context of handoff. The way channel switchings or the handoffs are managed in GSM network are not very different from what we discussed in a cellular network. So, our focus here is on the handoff procedure specific GSM. Handoff involves three basic steps, namely,

1. Signal measurements,

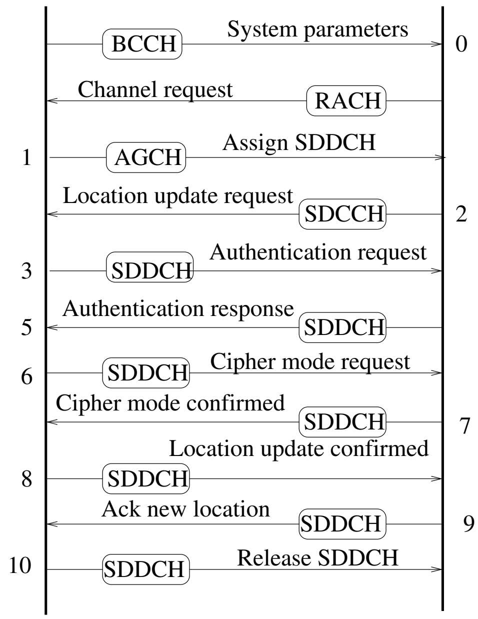


Figure 5.9: Channel activity needed for location update.

2. Handoff decision, and

3. Handoff execution.

Signal measurements report is transmitted periodically by MS. MS gather measurement values of 16 neighboring BSs and sends a report containing six strongest measurements over one of the 4 interleaved SACCHs. The handover decision and selection of target cell are made either by BSC or MSC. BSC makes a decision if the cell to which MS should be handed over is under its control. Otherwise BSC sends its global cell ID and a BSS map message for *handover request* to MSC. MSC then sends a BSS map message for *handover request* to new BSC. The message includes channel type and whether queueing is premissible or not.

The new BSC on receiving the request sends a BTSN channel activation message to its BS. It includes Handover Reference Number (HRN), handover type, channel number and type. Once BS's acknowledgement is received the new BSC sends acknowledgement to MSC's handover request message with HRN or handover reference number. MSC new responds to the old BSC

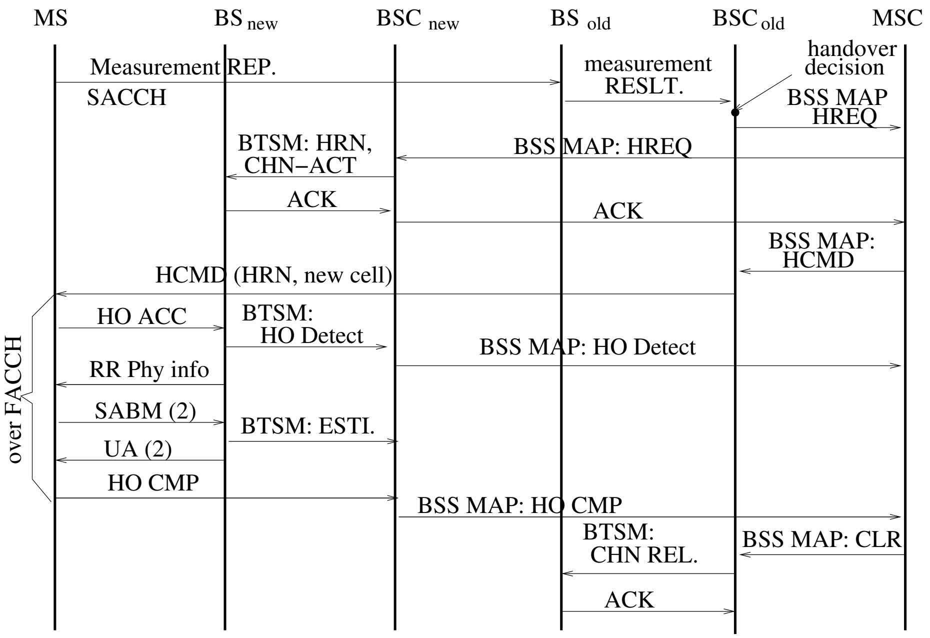


Figure 5.10: GSM inter BSC handover procedure.

with handover command. The old BSC in turn sends handover command to MS over FACCH. MS sends a handover access message to the new BS over FACCH. The new BS on the receipt of this message sends a BTSN handover detected message to the new BSC. The new BSC then sends BSS map handover detection message to the MSC. After this BS send physical information message providing the physical channels to be used for transmission by MS. MS responds by set asynchronous balance (SABM) layer-2 message to the new BS. The new BS then sends two messages one to the new BSC indicating link establishment and the other to MS which is a unnumbered answer layer-2 message.

The MS finally sends a handover complete message to the new BSC. The new BSC forwards the handover complete message to MSC. At this point handover is complete, so MSC sends a BSS map message asking the old BSC to clear radio resource used for MS. the old BSC sends a BTSM channel release message to the old BS. Once the old BS acknowledges the same, handover is complete. The entire process is illustrated by Figure 5.10.

In GSM, a intra-BSS handoffs due to channel switching within same cell or between cells under the coverage of same BSS may be handled independently by the BSS itself. But after performing an intra-BSS handoff, the BSS informs the MSC at the completion of the process. Intra BSC handover follows a process similar to inter BSC handover. Furthermore, channel switching may occur within same cell, between different cells under the coverage of a single BSS, or between cells under the coverage of different BSSs, and even different MSCs.

5.5 GPRS network

GSM is a circuit switched network that allows low speed data services. The transfer of data is allowed only during the time, the user occupies channel. Since data exchanges tend to be bursty, the circuit switched networks are unsuitable for large volume data transmission. A user has to pay for the entire duration of connection regardless of actual percentage of time the channel is actually engaged in transfer of data. General Packet Radio Service (GPRS) leverages GSM network to build a packet based mobile cellular network. It is architectured as an overlay network on GSM through a core IP based network consisting of two new nodes, some enhancements to BSS, certain software upgrades for HLR/VLR, and some new network interfaces. The new nodes that constitute the GPRS core network are Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). The upgrades for existing GSM nodes MSC, BTS, BSC, HLR and VLR are required to make them handle packetized data transfers. The BSC is connected to SGSN through frame relay link [**?**].

The two fundamental advantages of exchanging data on GPRS over that on GSM are:

1. Flow of data involving many users can be multiplexed and routed through multiple routes by packetizing data, and

2. Long latency for reconnection is eliminated by providing an *always on* connection.

Furthermore, by due to packetized data transfers, GPRS supports a data rate that is 3 times more than what can be supported by GSM network. The billing is done according to the number of packets transmitted by an individual user rather than the duration of connection time. By multiplexing data