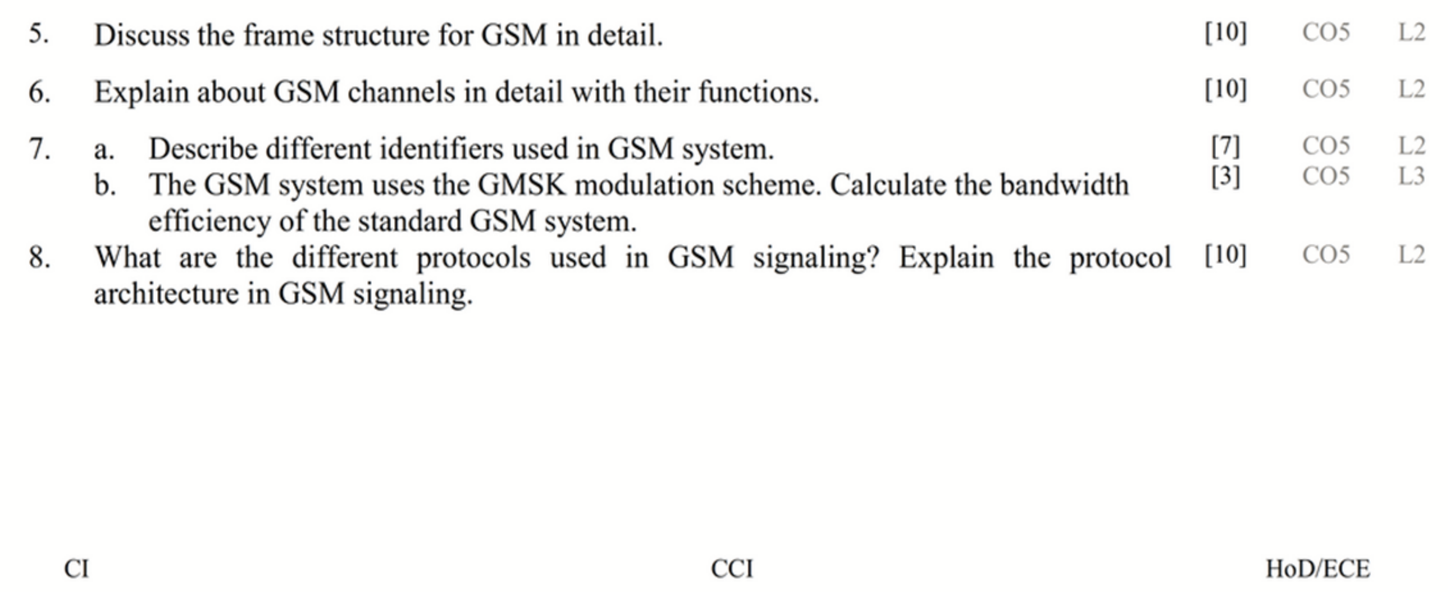
CMR
INSTITUTE OF
TECHNOLOGY

USN □□□□□□□□□□

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A++ GRADE BY NAAC

Internal Assessment Test-III									
Sub:	Optical and Wireless Communication							Code:	21EC72
Date:	17/12/2024	Duration:	90 mins	Max Marks:	50	Sem:	7th	Branch:	ECE(A,B,C,D)
Answer any **FIVE FULL** Questions									

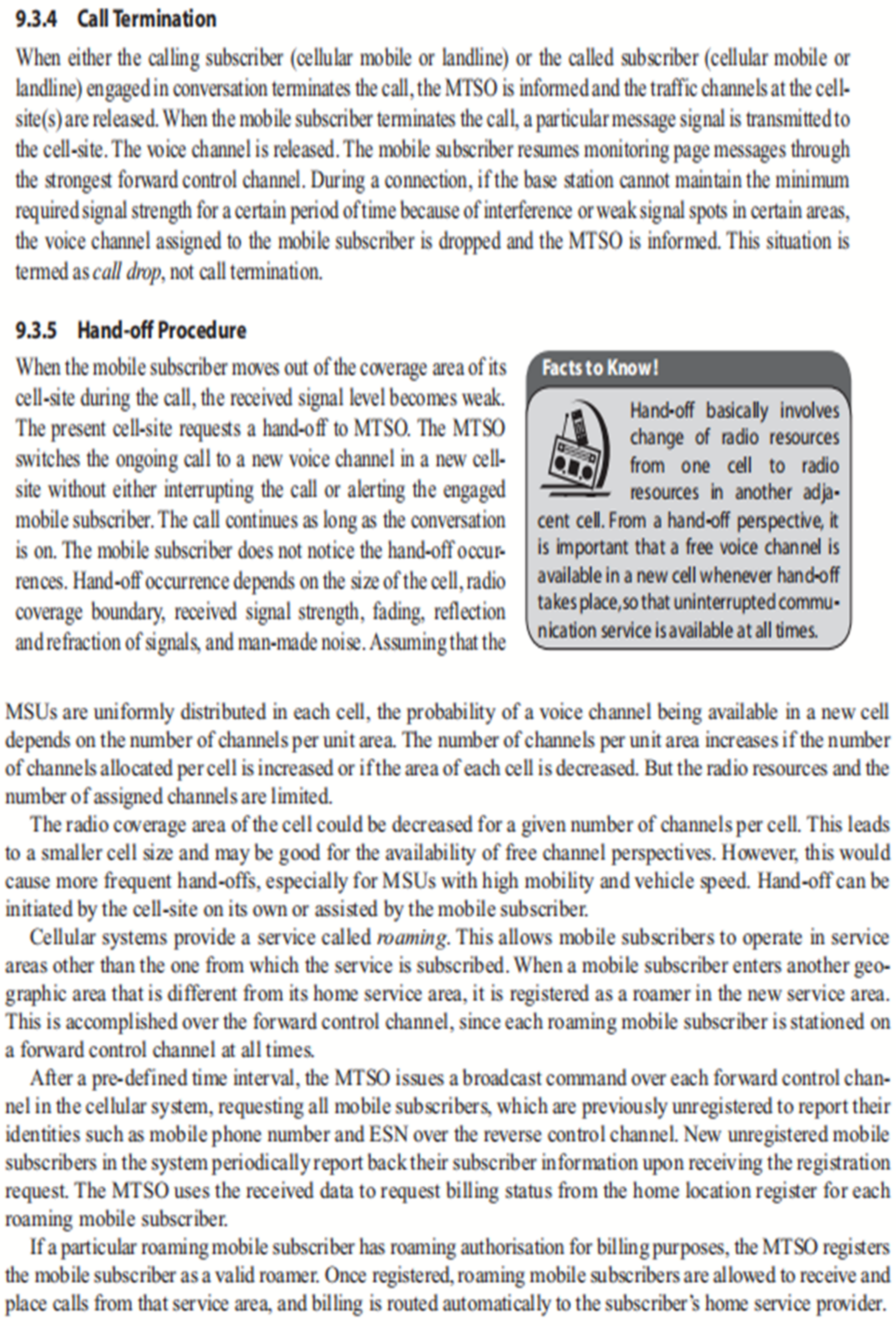
		Marks	OBE	
			CO	RBT
1.	Explain the following: a. Call drop and call termination. b. Handoff Procedure.	[10]	CO4	L2
2.	List and describe the essential components of a cellular telephone system.	[10]	CO4	L2
3.	Explain the various steps involved in placing a call from (a) Mobile to a landline phone (b) Landline phone to a mobile phone	[10]	CO4	L3
4.	Draw the GSM reference architectural model and explain briefly about all the GSM subsystem entities.	[10]	CO5	L2



5.	Discuss the frame structure for GSM in detail.	[10]	CO5	L2
6.	Explain about GSM channels in detail with their functions.	[10]	CO5	L2
7.	a. Describe different identifiers used in GSM system.	[7]	CO5	L2
	b. The GSM system uses the GMSK modulation scheme. Calculate the bandwidth efficiency of the standard GSM system.	[3]	CO5	L3
8.	What are the different protocols used in GSM signaling? Explain the protocol architecture in GSM signaling.	[10]	CO5	L2

CI CCI HoD/ECE

		Marks	CO	RBT
1.	Explain the following: a. Call drop and call termination. b. Handoff Procedure.	[10]	CO4	L2



9.3.4 Call Termination

When either the calling subscriber (cellular mobile or landline) or the called subscriber (cellular mobile or landline) engaged in conversation terminates the call, the MTSO is informed and the traffic channels at the cell-site(s) are released. When the mobile subscriber terminates the call, a particular message signal is transmitted to the cell-site. The voice channel is released. The mobile subscriber resumes monitoring page messages through the strongest forward control channel. During a connection, if the base station cannot maintain the minimum required signal strength for a certain period of time because of interference or weak signal spots in certain areas, the voice channel assigned to the mobile subscriber is dropped and the MTSO is informed. This situation is termed as *call drop*, not call termination.

9.3.5 Hand-off Procedure

When the mobile subscriber moves out of the coverage area of its cell-site during the call, the received signal level becomes weak. The present cell-site requests a hand-off to MTSO. The MTSO switches the ongoing call to a new voice channel in a new cell-site without either interrupting the call or alerting the engaged mobile subscriber. The call continues as long as the conversation is on. The mobile subscriber does not notice the hand-off occurrences. Hand-off occurrence depends on the size of the cell, radio coverage boundary, received signal strength, fading, reflection and refraction of signals, and man-made noise. Assuming that the MSUs are uniformly distributed in each cell, the probability of a voice channel being available in a new cell depends on the number of channels per unit area. The number of channels per unit area increases if the number of channels allocated per cell is increased or if the area of each cell is decreased. But the radio resources and the number of assigned channels are limited.

Facts to Know!

Hand-off basically involves change of radio resources from one cell to radio resources in another adjacent cell. From a hand-off perspective, it is important that a free voice channel is available in a new cell whenever hand-off takes place, so that uninterrupted communication service is available at all times.

The radio coverage area of the cell could be decreased for a given number of channels per cell. This leads to a smaller cell size and may be good for the availability of free channel perspectives. However, this would cause more frequent hand-offs, especially for MSUs with high mobility and vehicle speed. Hand-off can be initiated by the cell-site on its own or assisted by the mobile subscriber.

Cellular systems provide a service called *roaming*. This allows mobile subscribers to operate in service areas other than the one from which the service is subscribed. When a mobile subscriber enters another geographic area that is different from its home service area, it is registered as a roamer in the new service area. This is accomplished over the forward control channel, since each roaming mobile subscriber is stationed on a forward control channel at all times.

After a pre-defined time interval, the MTSO issues a broadcast command over each forward control channel in the cellular system, requesting all mobile subscribers, which are previously unregistered to report their identities such as mobile phone number and ESN over the reverse control channel. New unregistered mobile subscribers in the system periodically report back their subscriber information upon receiving the registration request. The MTSO uses the received data to request billing status from the home location register for each roaming mobile subscriber.

If a particular roaming mobile subscriber has roaming authorisation for billing purposes, the MTSO registers the mobile subscriber as a valid roamer. Once registered, roaming mobile subscribers are allowed to receive and place calls from that service area, and billing is routed automatically to the subscriber's home service provider.

2. List and describe the essential components of a cellular telephone system. [10] CO4 L2

9.2.2 Main Parts of a Basic Cellular System

A basic cellular system consists of mainly three parts: Cell-Site Equipment (CSE), Mobile Telephone Switching Office (MTSO), and Mobile Subscriber Unit (MSU) as shown in Fig. 9.2.

There is an air interface between the MSU and CSE. The interconnectivity between the CSE and MTSO, MTSOs, and the MTSO and PSTN is through wirelines or dedicated point-to-point microwave links.

Cell-Site Equipment (CSE) A cell-site is a fixed base station used for wireless communication with a mobile subscriber on one side as well as signaling/data communication with the MTSO on the other side. It is usually located at the centre or the edge of the coverage region of a cell. A cell-site consists of a number of transreceivers, *Tx*/*Rx* antennas mounted on a tall tower, data links, and power plant. The radio transmitting equipment operates at considerably higher RF power than do the mobile equipments. Tx power is shared among all the channels that are used at the cell-site. Similarly, there are as many receivers for each control and voice channel in use at the cell-site, as well as additional receivers for monitoring the signal strength of mobile subscribers in adjacent cells.

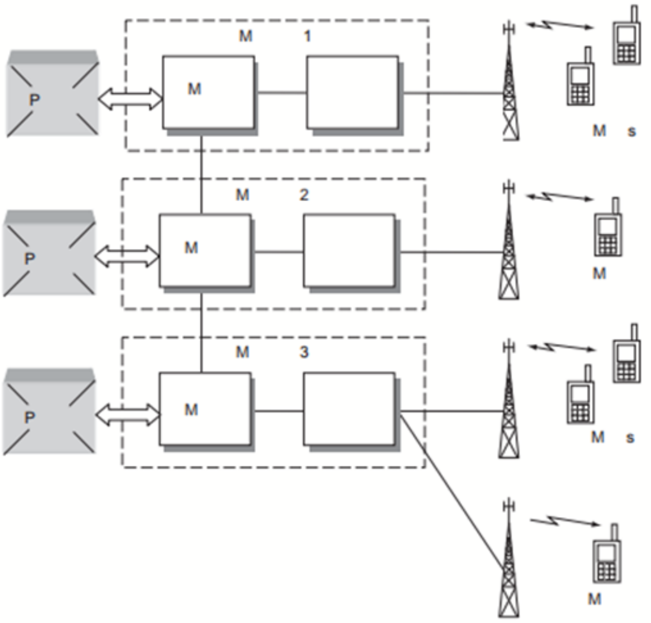


Fig.9.2 | *Parts of a basic cellular system*

Cell-site equipment basically comprises of two main parts—cell-site transceiver and cell-site controller. There may be adequate number of transceiver modules at the cell-site equipment in order to meet the subscriber capacity requirement within a cell. Data links are used to carry multiple-channel data from the cell-site to the MTSO. The transmission data rate on data links vary from 10 kbps to several Mbps. Many data-link channels can be multiplexed and passed through a wideband T-carrier (or E-carrier) wireline or a point-to-point microwave radio link operating at 850 MHz or higher frequency.

Radio transceivers are part of the cell-site equipment. The radio transceivers meant for voice channels can be either narrowband FM for analog systems or QAM/PSK modulation for digital systems with an effective audio-frequency band (approximately 300 Hz to 3000 Hz) comparable to a standard telephone circuit. The control channels use either FSK or PSK modulation scheme. The cell-site controller operates under the control of the central switching centre MSC or MTSO. The cell-site controller manages each of the radio channels at each cell-site, turns the radio transmitter and receiver on and off, transfers data onto the control and voice channels, monitors calls, and performs built-in diagnostic tests on the cell-site equipment.

The issues affecting the cellular system design in selection of cell-site antennas include antenna pattern, antenna gain, antenna tilting, and antenna height. The antenna radiation pattern can be omnidirectional, directional, or any other shape in both the horizontal and vertical planes. The antenna-radiation patterns are different as viewed in the cellular mobile operating environment from the antenna-radiation patterns as viewed in free space. Antenna gain compensates for the transmitted power. Antenna tilting can reduce the interference to the neighbouring cells and enhance the weak signal spots in the radio coverage of the cells. The height of the cell-site antenna can affect the area and shape of the coverage pattern in the cellular system.

Facts to Know!

The cell-site equipment is much more complex, bulky, and expensive than the individual mobile subscriber phones. Transmit and receive antennas may be separate antennas or combined ones at the cell-site. Generally, one Tx antenna and two Rx antennas are used at each cell-site or each sector.Two Rx antennas provide space diversity to counteract the effects of fading.

Mobile Telephone Switching Office (MTSO) It is the central coordinating element for all the cell-sites connected to it. It comprises of the switch and the processor. It also interfaces with the Public Switch Telephone Network (PSTN), controls call processing and handles billing activities. It uses voice trunks as well as data links between the cell-sites and the central processor. Microwave radio links or T-carriers (wirelines) carry both voice and data between the cell-site and the MTSO because the high-speed data link cannot be transmitted over the standard telephone trunks. The capacity of switching equipment in cellular systems is not based on the number of switch ports but on the capacity of the processor associated with the switches. The processor should be as large as possible. Also, it is important to consider when the switching equipment would reach the maximum capacity. It determines the service life of the switching equipment. More control modules can be added to increase the system capacity. Switching equipment can be linked to other switching equipments for better utilisation of hand-off.

The electronic switching centre located in the MTSO or MSC is a sort of digital telephone exchange that becomes the heart of a cellular telephone system. Electronic switches communicate with cell-site controllers using a data-link protocol, such as X.25, at a transmission rate of 9.6 kbps or higher. The electronic switching centre performs two essential functions:

- It controls switching between the public landline telephone network and the cell-site base stations for landline-to-mobile, mobile-to-landline, and mobile-to-mobile calls.
- It processes data received from the cell-site controllers concerning mobile subscriber status, diagnostic data, and bill-compiling information.

Mobile Subscriber Unit (MSU) Basically, a mobile subscriber unit comprises of a single antenna, transreceiver, and microprocessor-based control circuit. Because the cellular system is full duplex, the transmitter and receiver must operate simultaneously with a single antenna. A duplexer is used to separate the transmit and receive signals. The 45-MHz band separation between transmit and receive frequencies makes the operation relatively easy, and simplifies frequency synthesiser design.

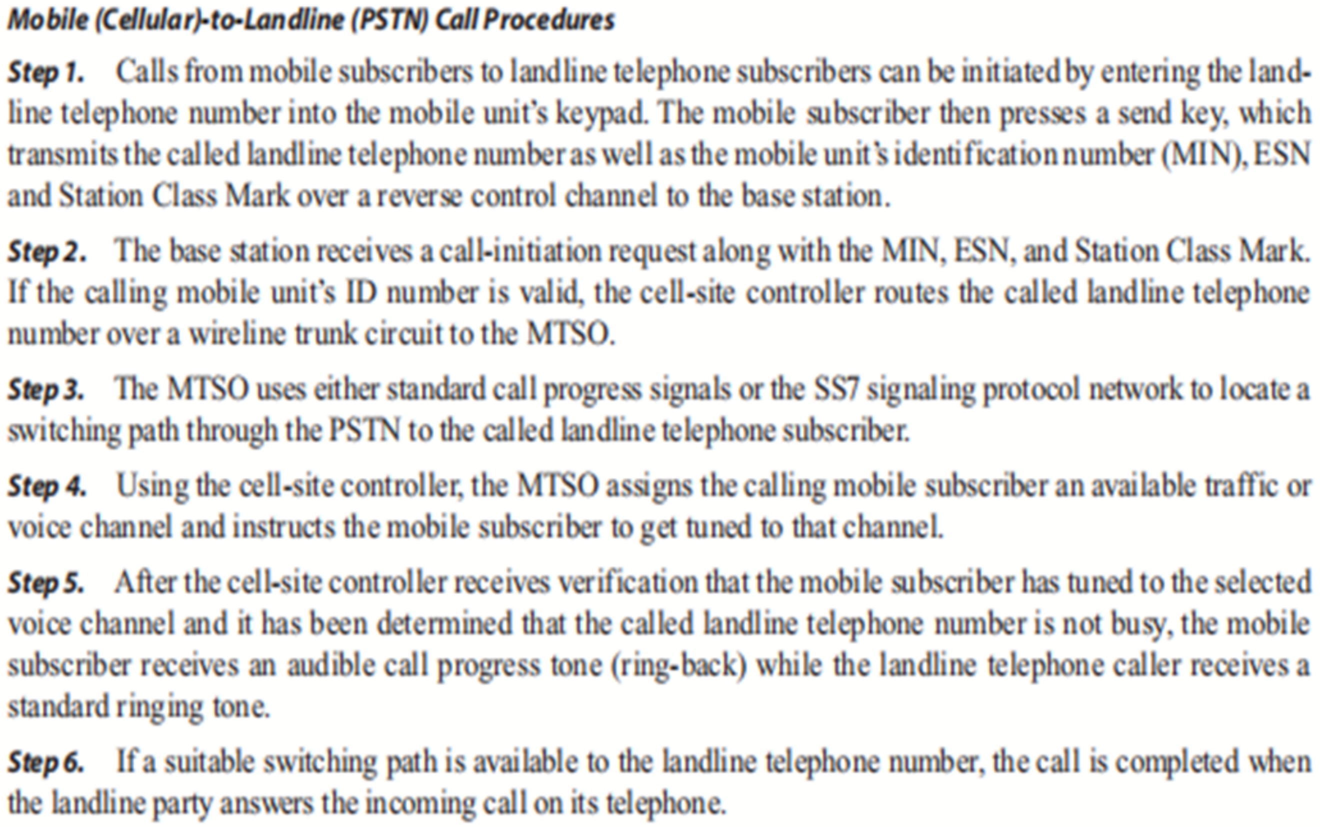
For example, GSM mobile subscriber comprises of two parts—the mobile equipment (ME) and an electronic smart card called a subscriber identity module (SIM). The ME is the hardware used by the subscriber to access the cellular network. The SIM is a card, which plugs into the ME. This card identifies the MS subscriber and also provides other information regarding the service that the subscriber should receive.

Each mobile subscriber consists of a mobile antenna, a multiple-frequency radio transceiver, and a control/logic unit. The transceiver uses a frequency synthesiser to tune into any designated cellular system channel. The control unit houses all the user interfaces, including a built-in handset or earphone or external microphone/speaker arrangement. The logic unit interrupts subscriber actions and system commands while managing the operation of the transceiver including transmit power.

Facts to Know !

Vehicle-installed mobile and portable/handheld mobile phone equipments are essentially identical except that portable/handheld mobile subscribers have a lower output power, have a less efficient antenna, and operate exclusively on batteries. Vehicle-installed mobile phone equipment have relatively large output power, have omnidirectional gain antenna mounted on the rooftop of the vehicle, and can operate from vehicle batteries.

3. Explain the various steps involved in placing a call from [10] CO4 L3
(a) Mobile to a landline phone
(b) Landline phone to a mobile phone



Mobile (Cellular)-to-Landline (PSTN) Call Procedures

Step 1. Calls from mobile subscribers to landline telephone subscribers can be initiated by entering the landline telephone number into the mobile unit's keypad. The mobile subscriber then presses a send key, which transmits the called landline telephone number as well as the mobile unit's identification number (MIN), ESN and Station Class Mark over a reverse control channel to the base station.

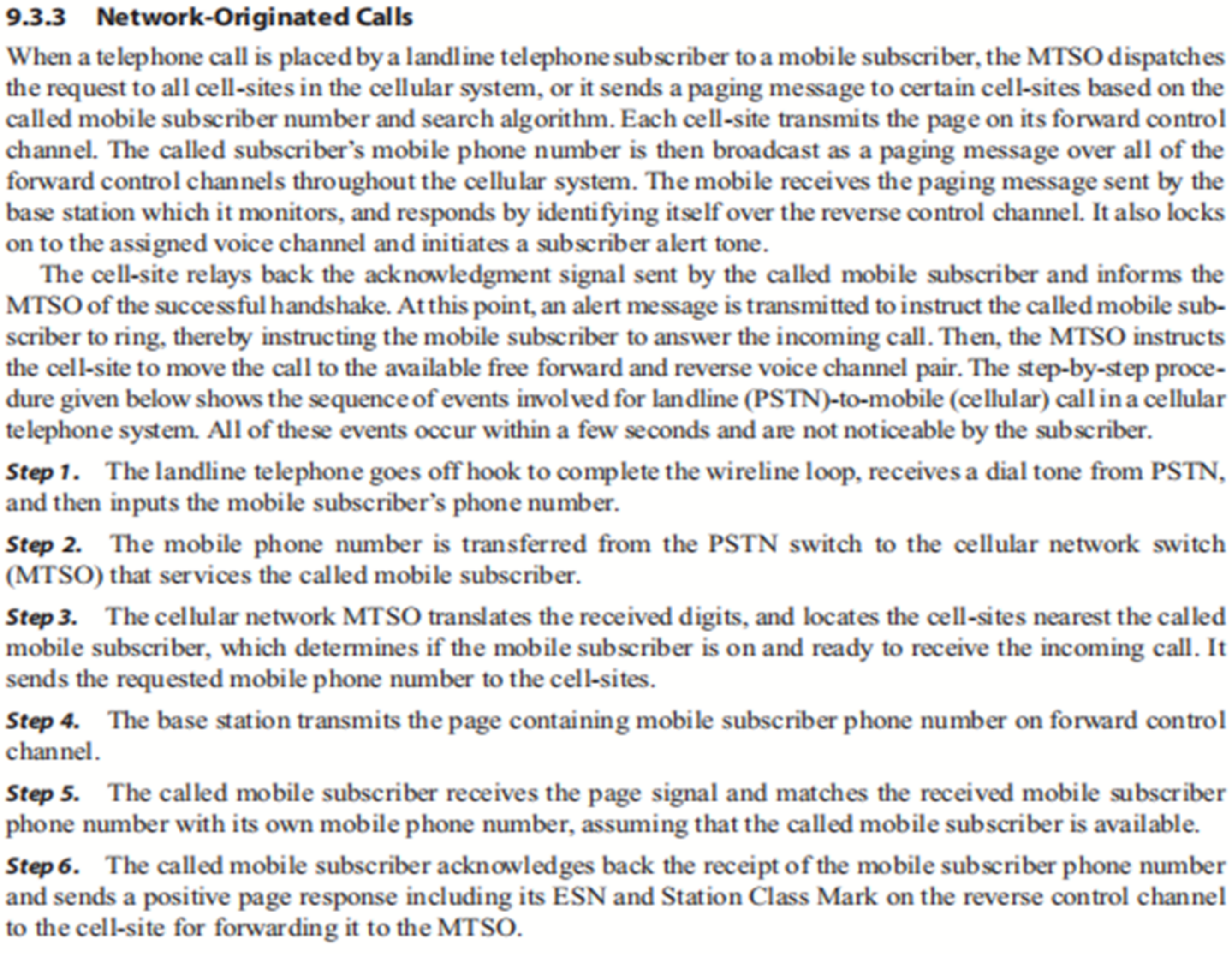
Step 2. The base station receives a call-initiation request along with the MIN, ESN, and Station Class Mark. If the calling mobile unit's ID number is valid, the cell-site controller routes the called landline telephone number over a wireline trunk circuit to the MTSO.

Step 3. The MTSO uses either standard call progress signals or the SS7 signaling protocol network to locate a switching path through the PSTN to the called landline telephone subscriber.

Step 4. Using the cell-site controller, the MTSO assigns the calling mobile subscriber an available traffic or voice channel and instructs the mobile subscriber to get tuned to that channel.

Step 5. After the cell-site controller receives verification that the mobile subscriber has tuned to the selected voice channel and it has been determined that the called landline telephone number is not busy, the mobile subscriber receives an audible call progress tone (ring-back) while the landline telephone caller receives a standard ringing tone.

Step 6. If a suitable switching path is available to the landline telephone number, the call is completed when the landline party answers the incoming call on its telephone.



9.3.3 Network-Originated Calls

When a telephone call is placed by a landline telephone subscriber to a mobile subscriber, the MTSO dispatches the request to all cell-sites in the cellular system, or it sends a paging message to certain cell-sites based on the called mobile subscriber number and search algorithm. Each cell-site transmits the page on its forward control channel. The called subscriber's mobile phone number is then broadcast as a paging message over all of the forward control channels throughout the cellular system. The mobile receives the paging message sent by the base station which it monitors, and responds by identifying itself over the reverse control channel. It also locks on to the assigned voice channel and initiates a subscriber alert tone.

The cell-site relays back the acknowledgment signal sent by the called mobile subscriber and informs the MTSO of the successful handshake. At this point, an alert message is transmitted to instruct the called mobile subscriber to ring, thereby instructing the mobile subscriber to answer the incoming call. Then, the MTSO instructs the cell-site to move the call to the available free forward and reverse voice channel pair. The step-by-step procedure given below shows the sequence of events involved for landline (PSTN)-to-mobile (cellular) call in a cellular telephone system. All of these events occur within a few seconds and are not noticeable by the subscriber.

Step 1. The landline telephone goes off hook to complete the wireline loop, receives a dial tone from PSTN, and then inputs the mobile subscriber's phone number.

Step 2. The mobile phone number is transferred from the PSTN switch to the cellular network switch (MTSO) that services the called mobile subscriber.

Step 3. The cellular network MTSO translates the received digits, and locates the cell-sites nearest the called mobile subscriber, which determines if the mobile subscriber is on and ready to receive the incoming call. It sends the requested mobile phone number to the cell-sites.

Step 4. The base station transmits the page containing mobile subscriber phone number on forward control channel.

Step 5. The called mobile subscriber receives the page signal and matches the received mobile subscriber phone number with its own mobile phone number, assuming that the called mobile subscriber is available.

Step 6. The called mobile subscriber acknowledges back the receipt of the mobile subscriber phone number and sends a positive page response including its ESN and Station Class Mark on the reverse control channel to the cell-site for forwarding it to the MTSO.

Step 7. The cell-site receives the mobile subscriber phone number, ESN, and Station Class Mark and passes the information to the MTSO.

Step 8. The MTSO verifies that the called mobile has a valid mobile subscriber phone number and ESN pair.

Step 9. The MTSO requests the cell-site controller to move the called mobile to the available pair of forward and reverse voice channels.

Step 10. The cell-site controller assigns an idle voice channel for the called mobile subscriber and the cell-site transmits the data message on the forward control channel for the called mobile subscriber to move to the specified voice channel.

Step 11. The called mobile subscriber receives the data messages on forward control channel to move to the specified voice channel and sends verification of designated voice channel to the cell-site.

Step 12. The cell-site controller sends an audible call progress tone to the called mobile subscriber, causing it to ring. The MTSO connects the called mobile subscriber with the calling landline phone on the PSTN. At the same time, a ring-back signal is sent back to the landline-calling telephone subscriber by PSTN.

Step 13. The called mobile subscriber answers back, the MTSO terminates the call-progress tones, and the two-way voice conversation begins on the forward voice channel and reverse voice channel between the calling telephone subscriber and the called mobile subscriber.

Once a call is in progress, the MTSO adjusts the transmitted power of the mobile subscriber and changes the channel of the mobile subscriber and cell-site in order to maintain call quality as the subscriber moves in and out of range of each cell-site. This is called hand-off procedure. Special control signaling is applied to the voice channels so that the cell-site may control the mobile subscriber while a call is in progress.

4. Draw the GSM reference architectural model and explain briefly about all the GSM subsystem entities. [10] CO5 L2

11.1 GSM NETWORK ARCHITECTURE

GSM uses two 25-MHz frequency bands, that is, the 890-MHz to 915-MHz band is used for mobile subscriber unit to base station transmissions (reverse-link transmissions), and the 935-MHz to 960-MHz frequency band is used for base station to mobile subscriber unit transmission (forward-link transmissions). GSM uses Frequency-Division Duplexing (FDD) and a combination of TDMA and FDMA techniques to provide simultaneous access to multiple mobile subscriber units.

Facts to Know!

The GSM system has an allocation of 50 MHz in the 900-MHz frequency band. Using FDMA, this band is divided into 124 RF channels, each with a carrier channel bandwidth of 200 kHz. Using TDMA, each of these carrier channels is further divided into 8 time slots. Thus, with the combination of FDMA and TDMA, a maximum of 992 channels can be realised for transmit and receive.

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 is 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 11.1 shows the key functional elements in the GSM network architecture.

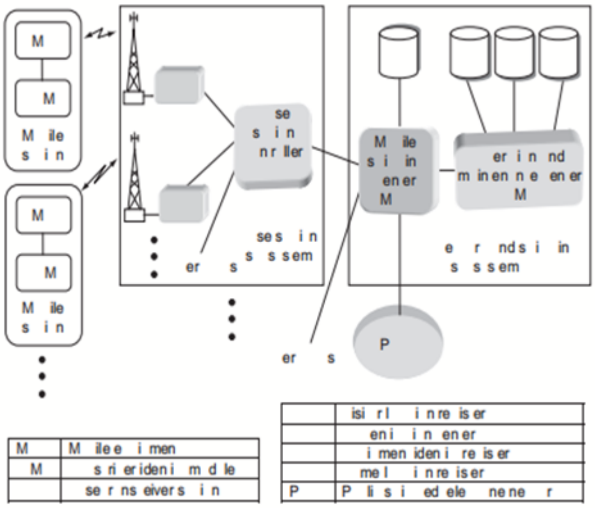


Fig. 11.1 | *GSM network architecture*

11.1.1 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 of 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 the transceiver, digital signal processors, and the antenna.

The second element of the MS in the GSM is the Subscriber Identity Module (SIM) that is a smart card issued at the subscription time identifying the specifications of a user such as a unique number and the type of service. The SIM card is unique to the GSM system. It is about postage-stamp size with 32 k bytes of memory that can be plugged into any GSM mobile phone. From the user's point of view, one of the most remarkable features of GSM is the SIM card, which is a portable device in the form of a smart card or plug-in module memory device that stores information such as the subscriber's identification number, privacy keys, the cellular networks and regions where the subscriber is authorised to service, and other user-specific information.

The GSM subscriber units are totally generic until a SIM is inserted. Therefore, a subscriber need only to carry a SIM card to use a wide variety of mobile equipments simply by inserting the SIM in the device to be used. In fact, except for certain emergency communications, the subscriber units will not work without a SIM inserted. Thus, the mobile equipment does not roam, it is the SIM which roams. The calls in the GSM are directed to the SIM inserted in any mobile phone. Short messages are also stored in the SIM card.

Facts to Know!

The Mobile Station is the technical name of the mobile or the cellphone. Although modern cellphones have become smaller and lighter, they are still called Mobile Stations as these were called so in early days due to their being bulky and sometimes installed in vehicles.

Facts to Know!

The 32 kbytes SIM card has inherent security features that make wireless transactions more secure than conducting transactions over the Internet.

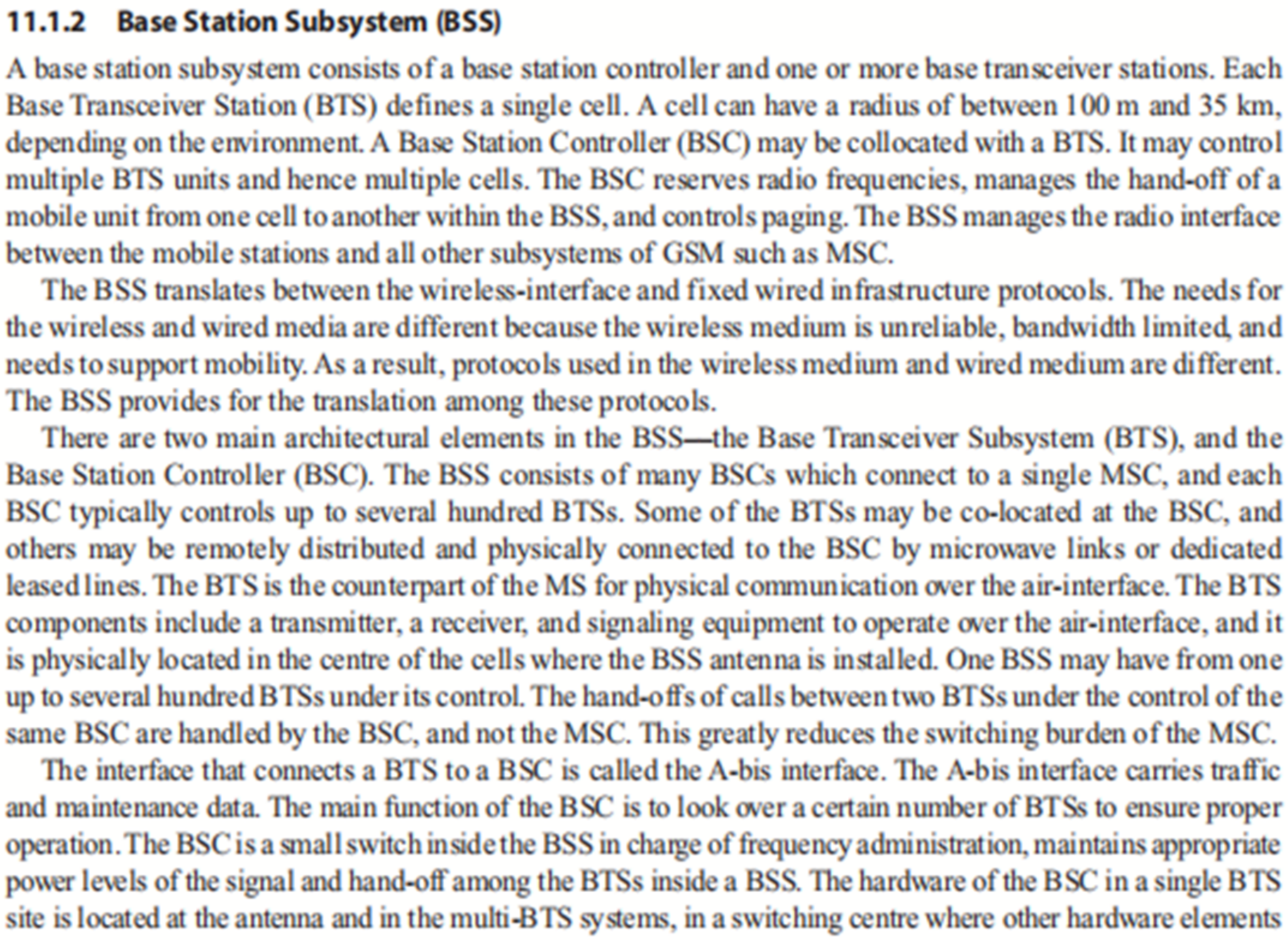
The SIM card allows a mobile subscriber to use any GSM mobile phone anywhere in the world where GSM services are available. Alternatively, people visiting different GSM-enabled countries that are not keen on making calls at their home number can always carry their own mobile phone and purchase a SIM card in any other country. This way they avoid roaming charges and the expense of having a different contact number. Several users can also share a mobile phone with different SIM cards.

Because SIM cards carry the private information for a user, a security mechanism is implemented in the GSM that asks for a four-digit PIN number to make the information on the SIM card available to the user. The SIM card also offers some protection against fraudulent use. A GSM mobile phone is useless without a SIM.

For example, if the mobile subscriber removes the SIM card when leaving the mobile phone in a vehicle, the mobile phone cannot be used unless another person has a valid SIM. Unfortunately, the SIM cards can be stolen too. The SIM can be set up to require the user to enter a Personal Identification Number (PIN) whenever the mobile phone is switched on to provide some security in case the card is lost or stolen.

Once a mobile phone user has a valid SIM, buying a new GSM mobile phone is easy. No set-up or programming is required. Similarly, a user can have a permanently vehicle-installed mobile phone and a handheld mobile phone with the same phone number, provided that only one is used at a time. The phone number of a mobile subscriber is usually of 10–15 digits. The first three digits are the country code; the next two are the digits for the specific MSC, and the rest are the telephone number. The IMSI of the same user is totally different from the ISDN telephone number. The first three digits of the IMSI identify the country, and the next two digits, the service provider.

Besides the SIM card, the next most 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 which changes with time for each user that is known only to the service provider.



11.1.2 Base Station Subsystem (BSS)

A base station subsystem consists of a base station controller and one or more base transceiver stations. Each Base Transceiver Station (BTS) defines a single cell. A cell can have a radius of between 100 m and 35 km, depending on the environment. A Base Station Controller (BSC) may be collocated with a BTS. It may control multiple BTS units and hence multiple cells. The BSC reserves radio frequencies, manages the hand-off of a mobile unit from one cell to another within the BSS, and controls paging. The BSS manages the radio interface between the mobile stations and all other subsystems of GSM such as MSC.

The BSS translates between the wireless-interface and fixed wired infrastructure protocols. The needs for the wireless and wired media are different because the wireless medium is unreliable, bandwidth limited, and needs to support mobility. As a result, protocols used in the wireless medium and wired medium are different. The BSS provides for the translation among these protocols.

There are two main architectural elements in the BSS—the Base Transceiver Subsystem (BTS), and the Base Station Controller (BSC). The BSS consists of many BSCs which connect to a single MSC, and each BSC typically controls up to several hundred BTSs. Some of the BTSs may be co-located at the BSC, and others may be remotely distributed and physically connected to the BSC by microwave links or dedicated leased lines. The BTS is the counterpart of the MS for physical communication over the air-interface. The BTS components include a transmitter, a receiver, and signaling equipment to operate over the air-interface, and it is physically located in the centre of the cells where the BSS antenna is installed. One BSS may have from one up to several hundred BTSs under its control. The hand-offs of calls 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.

The interface that connects a BTS to a BSC is called the A-bis interface. The A-bis interface carries traffic and maintenance data. The main function of the BSC is to look over a certain number of BTSs to ensure proper operation. The BSC is a small switch inside the BSS in charge of frequency administration, maintains appropriate power levels of the signal and hand-off among the BTSs inside a BSS. The hardware of the BSC in a single BTS site is located at the antenna and in the multi-BTS systems, in a switching centre where other hardware elements of NSS are located. The interface between a BSC and an MSC is called the A interface, which is standardised within GSM. The user's speech signal is converted into 13 kbps- digitised voice with a speech coder and communicated over the air-interface to provide a bandwidth efficient air-interface. The backbone wired network uses a 64 kbps PCM digitised voice in the PSTN hierarchy. Conversion from analog speech signal to 13 kbps digitised voice signal takes place at the mobile station, and the change from 13 kbps to 64 kbps coding takes place at the BSS. The call is established through the exchange of a number of packets.

11.1.3 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 Telecommunications Networks (PSTN or ISDN or Data Networks). The NSS controls hand-offs between cells in different BSSs, authenticates users and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. The NSS could be interpreted as a wireless specific switch that communicates with other switches in the PSTN and at the same time supports functionalities that are needed for a cellular mobile environment. The NSS interconnects to the PSTN through ISDN protocols. The NSS provides communications with other wired and wireless networks, as well as support for registration and maintenance of the connection with the MSs via BSCs in the radio subsystem.

The network and the switching subsystem together include the main switching functions of GSM as well as the databases needed for subscriber data and mobility management. In particular, the switching subsystem consists of

– Mobile Switch Centre (MSC)
– Home Location Register (HLR)
– Visitor Location Register (VLR)
– Authentication Centre (AuC)
– Equipment Identity Register (EIR)
– Interworking Function (IWF)

The NSS is the most elaborate element of the GSM network, and it has one hardware, Mobile Switching Centre (MSC), and four software database elements: Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identification Register (EIR), and Authentication Centre (AuC). An MSC is the hardware part of the wireless switch that can communicate with PSTN switches using the signaling system-7 (SS-7) protocol, as well as other MSCs in the coverage area of a service provider. If the MSC has an interface to the PSTN then it is called a Gateway MSC (GMSC). The MSC also provides the network the specific information on the status of the mobile terminals. The MSC basically performs the switching functions of the system by controlling calls to and from other telephone and data systems. It also does functions such as network interfacing and common channel signaling.Because the GSM represents an independent network, it must dispose of entities which provide connection to other users. Therefore, the main component of the switching subsystem is the Mobile Switching Centre, MSC. The main role of the MSC is to manage the communications between the GSM users and other telecommunications network users. The basic switching function is performed by the MSC, whose main function is to coordinate setting up calls to and from GSM users. The MSC has interfaces with the BSS on one side (through which MSC VLR is in contact with GSM users) and the external networks on the other side (ISDN/PSTN). An MSC is generally connected to several BSSs, which provide radio coverage to the MSC area. The MSC is also connected to other GSM Public Land Mobile Network (PLMN) entities such as other MSCs and HLR through a fixed network.

The MSC is the telephone switching office for mobile-originated or terminated traffic. The MSC controls the call set-up and routing procedures in a manner similar to the functions of a land network end office. The MSC provides call set-up, routing, and handover between BSCs in its own area and to/from other MSCs; an interface to the fixed PSTN; and other functions such as billing. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others.The HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber’s address, service type, current location, forwarding address, authentication/ciphering keys, and billing information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscriber Identity (IMSI) number that is totally different from the ISDN telephone number. The IMSI is used totally for internal networking applications. Each HLR is identified by the HLR number which is sent to all the required VLRs. The HLR is the reference database that permanently stores data related to subscribers, including a subscriber’s service profile, location information, and activity status. When an individual user buys a subscription from one of the GSM service providers, he is registered in the HLR of that service provider.Various identification numbers and addresses as well as authentication parameters, services subscribed, and special routing information are stored in the HLR. Current subscriber status, including a subscriber’s temporary roaming number and associated VLR if the mobile is roaming, are maintained. Location registration is performed by HLR.The HLR provides data needed to route calls to all MS-SIMs home based in its MSC area, even when they are roaming out of area or in other GSM networks. The HLR provides the current location data needed to support searching for and paging the MS-SIM for incoming calls, wherever the MS-SIM may be. The HLR is responsible for storage and provision of SIM authentication and encryption parameters needed by the MSC where theMS-SIM is operating. It obtains these parameters from the AuC. The HLR maintains records of which supplementary services each user has subscribed to and provides permission control in granting access to these services. Based on described functions, different types of data are stored in the HLR. Some data are permanent; that is, they are modified only for administrative reasons, while others are temporary and modified automatically by other network entities depending on the movements and actions performed by the subscriber. Some data are mandatory, other data are optional. Both the HLR and the VLR can be implemented in the same equipment in an MSC (collocated). A PLMN may contain one or several HLRs.The VLR is a 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 location of the mobile subscriber is determined by the VLR into which the mobile subscriber is entered. The visitor location register maintains information about mobile subscribers that are currently physically in the region covered by the switching centre. It records whether or not the subscriber is active and other parameters associated with the subscriber. For a call coming to the mobile subscriber, the system uses the mobile phone number associated to identify the home switching centre of the mobile subscriber. The home switching centre can find in its HLR the switching centre in which the mobile subscriber is presently located. For a call coming from the mobile subscriber, the VLR is used to initiate the call. Even if the mobile subscriber is in the area covered by its home switching centre, it is also represented in the switching centre’s VLR. A VLR is linked to one or more MSCs. The function of the VLR is to memorise temporarily information about the mobiles which are currently located in the geographical area controlled by the linked MSC. The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR supports a mobile paging-and-tracking subsystem in the local area where the mobile is presently roaming. The VLR is always integrated with the MSC. A VLR may be in charge of one or several MSC LAs (Location Areas). When a mobile subscriber roams from one LA to another, their current location is automatically updated in their VLR. When a mobile station roams into a new MSC area, if the old and new LAs are under the control of two different VLRs, the VLR connected to that MSC will request data about the mobile station from the HLR. The entry on the old VLR is deleted and an entry is created in the new VLR by copying the basic data from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call set-up without having to interrogate the HLR each time. The subscriber’s current VLR address, stored at the HLR, is also updated. This provides the information necessary to complete calls to roaming mobiles. These two databases, HLR and VLR, are used to keep track of the current location of an MS in GSM. Maintenance of two databases at home and at the visiting location allows a mechanism to support dialing and call routing in a roaming situation where the MS is visiting the coverage area of a different MSC. GSM transmission is encrypted. The AuC database holds different algorithms that are used for authentication and encryption of the mobile subscribers that verify the mobile user’s identity and ensure the confidentiality of each call. The AuC protects network cellular operators from different types of frauds and spoofing found in today’s cellular world. AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location registers. A stream cipher, A5, is used to encrypt the transmission from subscriber to base transceiver. However,the conversation is in the clear in the landline network. Another cipher, A3, is used for authentication. Different classes of SIM cards have their own algorithms, and the AuC collects all of these algorithms to allow the NSS to operate with different mobile terminals from different geographic areas.

The EIR is another database that keeps the information about the identity of mobile equipment such as 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.

Each mobile equipment is identified by IMEI which is memorised by the manufacturer and cannot be removed. By the registration mechanism the MS always sends the IMEI to the network, so that the EIR can memorise and assign them to three different lists:

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. Those phones are not able to enter in all the GSM networks which dispose of an EIR.

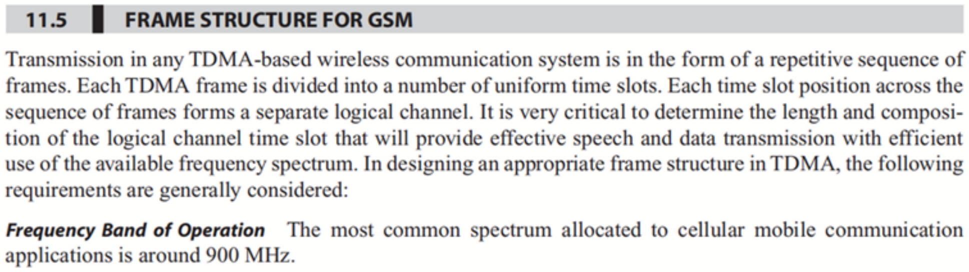
Grey List This list contains the IMEI of the phones momentarily not allowed to enter in the network, for example because the software version is too old or because they are in repair.

By the registration mechanism, the MSC checks if the MS is contained in the black or grey list; if so, the mobile cannot enter the network. One EIR per GSM network is enough. In the future there will be an interconnection between all the EIRs to avoid the situation where a mobile stolen in one country can be used in a GSM network from a different country. Both AuC and EIR can be implemented as individual stand-alone nodes or as a combined AuC/EIR node. The implementation of the EIR is left optional to the service provider.

IWF-Interworking Function It is a subsystem 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 conversion. The physical manifestation of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network.

The SS supports operation and maintenance of the system and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network. The OSS supports one or several Operation Maintenance Centres (OMC) that 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 to maintain all telecommunications hardware and network operations with a particular service area, manage all mobile equipment in the system, and manage all charging and billing procedures. 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 unit of mobile subscriber equipment in the system.

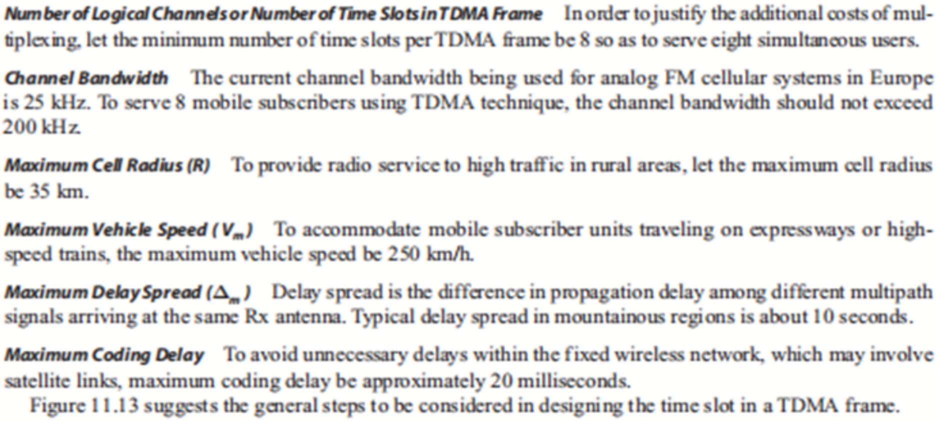
5. Discuss the frame structure for GSM in detail. [10] CO5 L2



11.5 FRAME STRUCTURE FOR GSM

Transmission in any TDMA-based wireless communication system is in the form of a repetitive sequence of frames. Each TDMA frame is divided into a number of uniform time slots. Each time slot position across the sequence of frames forms a separate logical channel. It is very critical to determine the length and composition of the logical channel time slot that will provide effective speech and data transmission with efficient use of the available frequency spectrum. In designing an appropriate frame structure in TDMA, the following requirements are generally considered:

Frequency Band of Operation The most common spectrum allocated to cellular mobile communication applications is around 900 MHz.



Number of Logical Channels or Number of Time Slots in TDMA Frame In order to justify the additional costs of multiplexing, let the minimum number of time slots per TDMA frame be 8 so as to serve eight simultaneous users.

Channel Bandwidth The current channel bandwidth being used for analog FM cellular systems in Europe is 25 kHz. To serve 8 mobile subscribers using TDMA technique, the channel bandwidth should not exceed 200 kHz.

Maximum Cell Radius (R) To provide radio service to high traffic in rural areas, let the maximum cell radius be 35 km.

Maximum Vehicle Speed (V_m) To accommodate mobile subscriber units traveling on expressways or high-speed trains, the maximum vehicle speed be 250 km/h.

Maximum Delay Spread (Δ_m) Delay spread is the difference in propagation delay among different multipath signals arriving at the same Rx antenna. Typical delay spread in mountainous regions is about 10 seconds.

Maximum Coding Delay To avoid unnecessary delays within the fixed wireless network, which may involve satellite links, maximum coding delay be approximately 20 milliseconds.

Figure 11.13 suggests the general steps to be considered in designing the time slot in a TDMA frame.

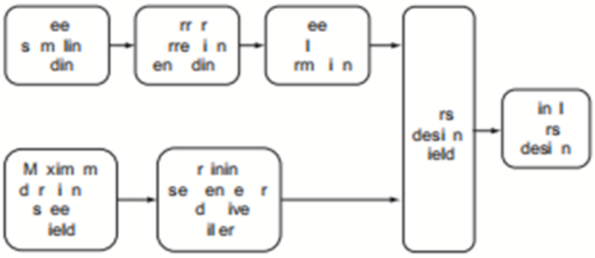


Fig. 11.13 | *Steps in design of TDMA time slot*

In the design of time slot of a TDMA frame, an appropriate data rate of the speech coder should be decided first. It is desirable that the speech coder must provide satisfactory speech quality at minimum data rate. The PCM speech coder has a data rate of 64 kbps, which is undesirably high for use with wireless systems. A data rate of 12 kbps is reasonable for reproducing good-quality speech. Since the coding delay is restricted to 20 milliseconds, the encoded speech can be formed into blocks of 20 ms duration. This converts the speech samples of 12 kbps × 20 ms = 240 bits.

Error correction can then be applied to the 240-bit blocks. Using a convolutional error-correcting technique with a code rate of , the number of bits in a block of 20-ms speech at 12 kbps rate increases to (2 × 240 bits =) 480-bits. With a constraint length of 5, 4 bits per block of 240 bits are added to account for the length of the shift register. This brings the speech block length to (480 + 2 × 8 =) 488 bits. With these parameters, the minimum bit rate for an eight-channel TDMA system can be computed as follows:

Number of bits in one channel = 488 bits
Number of channels or time sots = 8
Total number of bits in 8 time slots = 488 bits × 8 = 3904 bits
Duration of one speech block = 20 ms
Overall minimum channel bit rate =3904 bits/20 ms = 195.2 kbps

To take care of other design considerations, the gross channel bit rate will be slightly higher, and let it be greater than 200 kbps in the available channel bandwidth of 200 kHz. In a mobile radio environment, such data rates can be achieved with the use of adaptive equalisation. Adaptive equalisation will require the inclusion of a new training sequence in each time slot when the mobile subscriber moves a sufficient distance to potentially cause changes in the characteristics of transmission path. Assume that the phase angle of the carrier signal changes by λ_c /20 of the maximum vehicle speed. Thus, at 900 MHz ($\lambda_c = 0.333$m), we have

Maximum transmission duration (one-way) = $(\lambda_c/20)/V_m$
Maximum transmission duration (one-way) = (0.333m/20)/250 km/h
Maximum transmission duration (one-way) = 0.24 ms
Or, Maximum transmission duration (two-way) = 2 × 0.24 = 0.48 ms
Hence, Duration for data transmission in a time slot, $_d$= 0.48 ms

Assuming the number of taps on the adaptive equaliser to be equal to 6 times the number of bits transmitted in the maximum dispersal time ($\Delta_m = 0.01$ ms), the amount of time needed for the training sequence in the time slot, $_t$ = 0.06 ms.

To account for the differing amounts of delay between different mobile units and the base station, a guard interval is needed at the end of each time slot. Because eight mobile subscriber units share the same TDMA frame, it is necessary to adjust the timing of the transmissions of the mobile subscriber units so that the transmission from one mobile subscriber does not interfere with adjacent time slots. The guard time can be computed as follows.

Let the average duration of the voice call = 120 seconds
Maximum vehicle speed of the mobile = 250 km/h

Therefore, the radial distance a mobile moving toward or away from the base station located at the centre of the cell = (250 km/h) × (120 s) = 8333 m

The change in propagation delay = 8333 m/(3×10^8 m/s) ≈ 0.03 ms
Or, Required duration for guard interval, $_g$ = 0.03 ms

Figure 11.14 shows the tentative design of a time slot, depicting time duration of two blocks of data before and after the training sequence and guard time.

So, Maximum time duration of a time slot, $T_s = T_d + T_{ts} + T_g$
Maximum time duration of a time slot, T_s = 0.48 ms + 0.06 ms + 0.03 ms
Maximum time duration of a time slot, T_s = 0.57 ms
Number of time sots in a TDMA frame = 8
Duration of a TDMA frame = 8 × 0.57 ms = 4.6 ms

This is quite close to actual design of a TDMA time slot and frame structure used in GSM. Fundamentally, each 200-kHz frequency band is divided into 8 logical channels defined by the repetitive occurrence of time slots. The GSM system uses the TDMA scheme shown in Fig. 11.15 with a 4.615 ms-long frame, divided into eight time slots each of 557 μs. Each frame is 156.25 bits long, of which 8.25 bits are guard bits.

At the lowest level is the time slot or a burst period, which has a duration of approximately 577 μs. With a bit rate of 270.833 kbps, each time slot has a length of 156.25 bits. The time slot includes the following fields:

Tail Bits, T (3 Bits each at the Beginning and End of a Time Slot Excluding Guard Bits) It allows synchronisation of transmissions from mobile units located at different distances from the base station.

Encrypted Data (114 Bits) Data is encrypted in blocks by conventional encryption of 114 plaintext bits into 114 ciphertext bits; the encrypted bits are then placed in two 57-bit data fields in the time slot.

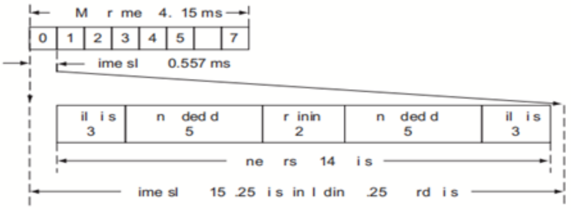


Fig. 11.15 GSM basic frame structure

Stealing Bit, S (1 Bit each at the End of Two 57-Bit Data Fields in the Time Slot) It is used to indicate whether this block contains data or is stolen for urgent control signaling purpose during the call.

Training Data (26 Bits) It is used to adapt the parameters of the receiver to the current path-propagation characteristics and to select the strongest signal in case of multipath propagation. The training sequence is a known bit pattern that differs for different adjacent cells. It enables the mobile subscriber units and base stations to determine that the received signal is from the desired base station and not from a strong interfering base station. In addition, the training sequence is used for multipath equalisation, which is used to extract the desired signal from unwanted reflections.

Guard Bits, G (8.25 Bits) It is used to avoid overlapping with other bursts due to different path delays.

The 148 bits of a data burst are used to transmit the information. Delimited by tail bits (consisting of 0s), the frame contains 26 training bits sandwiched between two bursts of data bits. These training bits allow the receiver to synchronise itself.

Moving up the frame format hierarchy, 8-time slots TDMA frames are typically organised into a 26-frame multiframe. One of the frames in the multiframe is used for control/signaling and another is currently unused, leaving 24 frames for data traffic. Thus, each traffic channel receives one slot per frame and 24 frames per 120-ms multiframe.

The gross channel data rate can be calculated as follows:

$$\text{Number of data bits per time slot} = 114 \text{ bits}$$
$$\text{Number of time slots per multiframe} = 24$$
So, $$\text{Number of bits per multiframe} = 24 \times 114 \text{ bits} = 2736 \text{ bits}$$
$$\text{Time duration of one multiframe} = 120 \text{ ms}$$
So, $$\text{Gross data rate} = 2736 \text{ bits}/120 \text{ ms} = 22.8 \text{ kbps}$$

GSM uses a complex hierarchy of TDMA frames to define logical channels, as shown in Fig. 11.16.

The GSM specification also allows half-rate traffic channels, with two traffic channels each occupying one time slot in 12 of the 26 frames. With the use of half-rate speech coders, this effectively doubles the capacity of the system. There is also a 51-frame multiframe used for control traffic. Thus, many frames are combined to constitute multiframe, superframe, and hyperframes.

11.5.1 Physical Data Bursts in GSM

Each user transmits a burst of data during the time slot assigned to it. GSM supports five types of packet data bursts used for control and traffic signaling.

The normal burst, shown in Fig. 11.17, is used for TCH and DCCH transmissions on both the forward and reverse link.

The normal burst consists of three bits each at the beginning and at the end of the data burst, 8.25 bits of guard period, two sets of 58 bits encrypted bits (a total of 116 bits), and a 26-bits training sequence.

r is 3	n r ed d 5	r inin is 2	n r ed d 5	is 3	rd eri d .25 is

Fig. 11.17 | *The normal data burst in GSM*

The start bits are 000 providing a gap time for the digital radio circuitry to cover the uncertainty period to ramp on and off for the radiated power and to initiate the convolutional decoding of the data. The 26-bit training sequence is used to train the adaptive equaliser at the receiver. The training of the equaliser is in the middle of the burst because the channel behaviour is constantly changing during the transmission of the data burst. The 116 encrypted data bits include 114 bits of data and two flag bits at the end of each part of the data that indicates whether data is user traffic or signaling and control information during the call.

The Frequency-Correction (FCCH) burst is used in TS 0 of specific frames to broadcast the frequency synchronisation control messages by the BTS on the forward link. MSs use it to synchronise with the master clock in the system. The frame format of the FCCH data burst is shown in Fig. 11.18.

r is 3	ixed is ll 0s 142	is 3	rd eri d .25 is

Fig. 11.18 | *The FCCH data burst in GSM*

The FCCH burst has three bits at the start and the end of the data field. The rest of the data burst contains all 0s that allows transmission of the unmodulated carrier frequency. Guard period equivalent to 8.25-bits duration is used between two bursts.

The synchronisation (SCH) burst, as shown in Fig. 11.19, is very similar to the normal burst except that the training sequence is longer and the coded data are used for the specific task of identifying the network. The SCH burst is used in TS 0 of specific frames to broadcast the frequency and time synchronisation control messages on the forward link.

r is 3	n r ed d 3	r inin is 4	n r ed d 3	is 3	rd eri d .25 is

Fig. 11.19 | *The SCH data burst in GSM*

The BTS broadcasts the SCH burst, and the MSs use it for initial training of the equaliser, initial learning of the network identity and to synchronise the time slots.

The random access (RACH) burst, as shown in Fig. 11.20, is used by the MS to access the BS as it registers to the network.

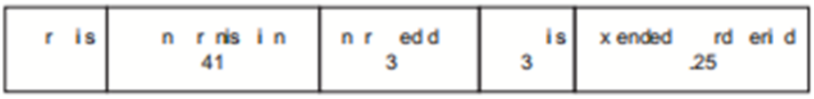


Fig. 11.20 | *The RACH data burst in GSM*

The overall structure of the RACH data burst is similar to the normal data burst except that a longer start bits and synchronisation sequence is used to initiate the equaliser. A much longer guard period of 68.25 bits allows approximate estimation of the distance of the MS from its serving BTS. The distance can be computed from the arrival time of the RACH burst. A guard period of 68.25 bits translates to 252 μs. The signal transmitted from a MS should travel more than 75.5 km (at the signal speed of 300,000 km/sec) before arriving at the BTS to exceed this guard period.

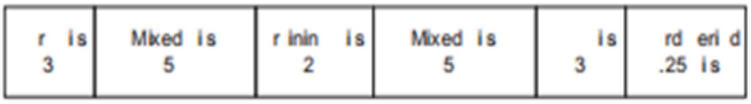


Fig. 11.21 | *The dummy burst in GSM*

The dummy burst, as shown in Fig. 11.21, is used as filler information for unused time slots on the forward link.

The Concept of Time Slot in GSM Channel A time slot consists of 156.25 bits that are transmitted at a rate of 270.833 kbps. In one time slot, 114 bits are encrypted data bits transmitted as two times 57 data bits each. The training sequence in the middle of the time slot consists of 26 bits. It allows the adaptive equaliser in the receivers of the base station and mobile unit to analyse the characteristics of the wireless channel before decoding the user data. On either side of the training sequence, there are control bits called stealing flags. The bit value of these two flags distinguishes the time slot to contain either the voice or control information during the call.

The Concept of TDMA Frames in GSM Channel During a frame, one time slot is used to transmit only and another time slot is used to receive only. The remaining six time slots of a frame can be used to measure received signal level from its serving base station as well as that from up to five adjacent base stations.

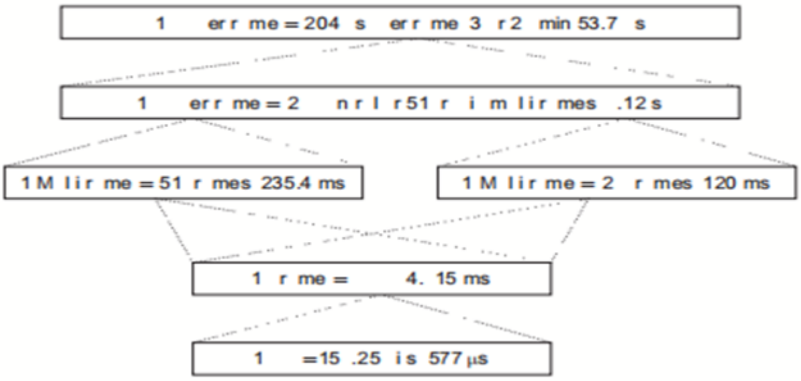

1 err me = 204 s err me 3 r 2 min 53.7 s
1 err me = 2 n r l r 51 r i m lir mes .12 s
1 M lir me = 51 r mes 235.4 ms
1 M lir me = 2 r mes 120 ms
1 r me = 4. 15 ms
1 =15 .25 is 577 μs

Fig. 11.23 | *GSM frame hierarchy*

The GSM radio-interface standard provides a variety of control channels and traffic channels defined in a hierarchy built upon the basic eight-slot TDMA transmission format. The frame hierarchy, depicted in Fig. 11.23, shows the TDMA hierarchy of the GSM network from a normal data burst of 577 μs interval to a hyperframe of length of around three-and-half hours.

The basic building block of the GSM frame hierarchy is a 4.615-ms TDMA frame. Each frame comprises of eight data bursts or time slots. The time-slot interval is equivalent to the transmission time for about 156.25 bits, comprising of 114 bits user data and the remaining overhead bits. A TDMA frame contains 8 × 156.25 bits = 1250 bits. The frame rate is 270.833 kbps/1250 bits/frame = 216.66 frames per second.

The Concept of Multiframes in GSM Channel Each of the normal speech frames are grouped into larger structures called multiframes, superframes and hyperframes. The 13th or 26th frames are used for control data only. Each 120-ms multiframe is composed of 26 frames—24 frames carry user information, and two frames carry system control information related to individual users. The gross data rate per user is 24 × 114 bits / 120 ms = 22.8 kbps. The speech coder has a net data rate of 13 kbps, and the addition of error-correction coding results into gross transmission data rate up to 22.8 kbps per user. The eight-slot TDMA frames may be also organised into control multiframes. Control multiframes are used to establish several types of signaling and control channels used for system access, call set-up, synchronisation, and other system control functions. The control multiframes span 51 TDMA frames.

The Concept of Superframes in GSM Channel Either traffic or control multiframes are grouped into superframes, which are in turn grouped into hyperframes. One traffic multiframe contains 26 frames, and one traffic superframe contains 51 traffic multiframes, or 1326 frames. A hyperframe contains 2048 superframes, or 2,715,648 frames. A complete hyperframe takes about every 3 hours, 28 minutes, and 54 seconds. The encryption algorithms rely on the particular frame number, and sufficient security can only be obtained by using a large number of frames as provided by the hyperframe. Counters at the mobile subscribers need to track the frame numbers at hyperframe, superframe, and multiframe levels to communicate with the network.

6. Explain about GSM channels in detail with their functions. [10] CO5 L2

11.4 GSM CHANNELS

GSM-900 has been allocated an operational frequency from 890 MHz to 960 MHz. GSM uses the frequency band 890 MHz–915 MHz for uplink (reverse) transmission, and for downlink (forward) transmission, it uses the frequency band 935 MHz–960 MHz. The available 25-MHz spectrum for each direction is divided into 124 Frequency Division Multiplexing (FDM) channels, each occupying 200 kHz with 100 kHz guard band at two edges of the spectrum. This is shown in Fig. 11.10.

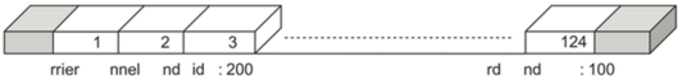


Fig. 11.10 *Frequency channels in GSM-900*

GSM uses FDD and a combination of TDMA and FDMA schemes to provide multiple access to mobile subscribers. The available forward and reverse frequency bands are divided into 200-kHz wide channels called ARFCNs (Absolute Radio Frequency Channel Numbers). The ARFCN denotes a forward and reverse channel pair that is separated in frequency by 45 MHz and each channel is time shared between as many as eight subscribers using TDMA.

The total number of available channels within a 25-MHz bandwidth is 125 (assuming no guard band). Since each radio channel consists of eight time slots, there are thus a total of 1000 traffic channels within a GSM. In practical implementations, a guard band of 100 kHz is provided at the upper and lower end of the GSM spectrum, and only 124 channels are available for use.

Each carrier supports eight time slots for the TDMA operation. Each of the eight subscribers uses the same ARFCN and occupies a unique Time Slot (TS) per frame. A guard frame of 8.25 bits is used in between any two frames transmitted either by the BS or the MS. The data rate of each carrier is 270.833 kbps that is provided with a modulation scheme known as GMSK (Gaussian Minimum Shift Keying) that is a variant of FSK having a frequency deviation of ± 67.71 kHz. The channel data rate of GSM is 270.833 kbps, which is exactly four times the RF frequency shift. This minimises the bandwidth occupied by the modulation spectrum and hence improves channel capacity. The MSK modulated signal is passed through a Gaussian filter to smooth the rapid frequency transitions that would otherwise spread energy into adjacent channels. The bandwidth-time product ($B \times T_b$) of GMSK is standardised at 0.3, a normalised bandwidth expansion factor where 0.3 describes the 3 dB bandwidth of the Gaussian pulse shaping filter with relation to the bit rate, which provides the best compromise between increased bandwidth occupancy and resistance to cochannel interference. Ninety-nine per cent of the RF power of GMSK signals so specified is confined to a bandwidth of 250 kHz, which means that, for all practical purposes, the sidelobes of the GMSK signal are insignificant, and outside this frequency band.

With the channel data rate of 270.833 kbps, the duration of each bit is 3.69 μs, and the effective channel transmission rate per user is 33.854 kbps (270.833 kpbs/8 users). With overhead, user data is actually transmitted at a maximum rate of 24.7 kbps. The user transmission packet burst is fixed at 577 μs, which accommodates information bits and a time gap between the packets for duration equivalent to 156.25 channel bits times the bit duration of 3.69 μs.

GSM employs a moderately complicated, 13-kbps regular pulse-excited speech codec (coder/decoder) with a long-term predictor. To provide error protection for the speech-encoded bits, concatenated convolutional codes and multilayer interleaving are employed. An overall speech delay of 57.5 ms occurs in the system.

11.4.1 GSM Logical Channels

The combination of a time slot number and an ARFCN constitutes a physical channel for both the forward and reverse links. Each physical channel in a GSM system can be mapped into different logical channels at different times. That is, each specific time slot or frame may be dedicated to either handling traffic data (user data such as speech, facsimile, or teletext data), signaling data, or control channel data (from the MSC, base station, or mobile subscriber).

Communication between the mobile subscriber and the base station is involved with both voice as well as signaling and control. Voice and signaling packets are inserted in a hierarchy and mobile subscribers use counters to identify the location of specific packet bursts in the overall structure of the frames. The entire communication system can be thought of as a distributed real-time computer that uses a number of instructions to transfer information packets from one location to another. Initial signaling is needed for registration and call establishment, followed by maintaining the synchronisation among the mobile subscribers, mobility management, and need to transfer the data traffic.

There is a need of a set of instructions and ports to instruct different elements of the cellular network to perform their specified duties. In cellular communication systems, these ports are referred to as logical channels. Logical channels use a physical TDMA slot or a portion of a physical slot to specify an operation in the network in GSM. GSM uses a variety of multiplexing techniques to create a collection of logical channels.

The GSM specification defines a wide variety of logical channels that can be used to link the physical layer with the data link layer of the GSM network. These logical channels efficiently transmit user data while simultaneously providing control of the network on each ARFCN. GSM provides explicit assignments of time slots and frames for specific logical channels. The logical channels used by a GSM system are shown in Table 11.2.

Table 11.2 *Logical channels in GSM*

Channel type	*Channel group*	*Channel*	*Direction*
Control Channel (CCH)	Broadcast Channel (BCH)	Broadcast Control Channel (BCCH)	Downlink (BS → MS)
		Frequency Correction Channel (FCCH)	Downlink (BS → MS)
		Synchronisation Channel (SCH)	Downlink (BS → MS)
	Common control Channel (CCCH)	Paging Channel (PCH)	Downlink (BS → MS)
		Random Access Channel (RACH)	Uplink (MS → BS)
		Access Grant Channel (AGCH)	Downlink (BS → MS)
	Dedicated control Channel (DCCH)	Standalone Dedicated Control Channel (SDCCH)	Uplink and Downlink (BS ↔ MS)
		Slow Associated Control Channel (SACCH)	Uplink and Downlink (BS ↔ MS)
		Fast Associated Control Channel (FACCH)	Uplink and Downlink (BS ↔ MS)
Traffic Channel (TCH)	Traffic Channel (TCH)	Full-rate Traffic Channel (TCH/F)	Uplink and Downlink (BS ↔ MS)
		Half-rate Traffic Channel (TCH/H)	Uplink and Downlink (BS ↔ MS)

The logical channels in the GSM network are divided into two principal categories: Control Channels (CCHs) and Traffic Channels (TCHs). Control channels carry signaling and synchronising commands between the base station and the mobile station. Certain types of control channels are defined for just the forward or reverse link. Traffic channels carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link. GSM system uses a variety of logical control channels to ensure uninterrupted communication between MSs and the BS.

11.4.2 GSM Control Channels

There are three classes of control channels defined in GSM: Broadcast Channels (BCH), Common Control Channels (CCCH), and Dedicated Control Channels (DCCH). Each control channel consists of several logical channels that are distributed in time to provide the necessary GSM control functions.

Facts to Know!

The BCH and CCCH forward control channels in GSM are implemented only on certain ARFCN channels and are allocated time slots in a very specific manner.

Specifically, the BCH and CCCH forward control channels are allocated only TS 0 and are broadcast only during certain frames within a repetitive fifty-one frame sequence (called the control channel multiframe) on those ARFCNs which are designated as broadcast channels. TS1 through TS7 carry regular TCH traffic, so that ARFCNs that are designated as control channels are still able to carry full-rate users on seven of the eight time slots.

The GSM specification defines thirty-four ARFCNs as standard broadcast channels. For each broadcast channel, the frame number 51 does not contain any BCH/CCCH forward channel data and is considered to be an idle frame. However, the reverse channel CCCH is able to receive subscriber transmissions during TS 0 of any frame (even the idle frame). On the other hand, DCCH data may be sent during any time slot and any frame, and entire frames are specifically dedicated to certain DCCH transmissions.

The BCH channels are broadcast from the BTS to MSs in the coverage area of the BTS, and thus are one-way channels. The broadcast channel operates on the forward link of a specific ARFCN within each cell, and transmits data only in the first time slot (TS 0) of certain GSM frames. The BCH provides synchronisation for all mobiles within the cell and is occasionally monitored by mobiles in neighbouring cells so that received power and MAHO decisions may be made by out-of-cell users. Although BCH data is transmitted in TS 0, the other seven time slots in a GSM frame for that same ARFCN are available for TCH data, DCCH data, or are filled with dummy bursts. Furthermore, all eight time slots on all other ARFCNs within the cell are available for TCH or DCCH data. There are three separate broadcast channels that are given access to TS 0 during various frames of the 51-frame sequence.

(a) The Broadcast Control Channel (BCCH) is used by BTS to broadcast system parameters such as the frequency of operation in the cell, operator identifiers, cell ID, and available services to all the MSs. Once the carrier, bit, and frame synchronisation between the BTS and MS are established, the BCCH informs the MS about the environment parameters associated with the BTS covering that area such as current control channel structure, channel availability, and congestion. The BCCH also broadcasts a list of channels that are currently in use within the cell. Frames 2 through frame 5 in a control multiframe (4 out of every 51 frames) contain BCCH data. The BCCH is physically implemented over the Normal Burst (NB). The BCCH is also a continuously keyed channel, and it is used for signal strength measurements for hand-off.

(b) The Frequency Correction Control Channel (FCCH) is used by the BTS to broadcast frequency references and frequency correction burst of 148 bits length. An MS in the coverage area of a BTS uses the broadcast FCCH signal to synchronise its carrier frequency and bit timing. The FCCH is a special data burst that occupies TS 0 for the very first GSM frame (Frame 0) and is repeated every ten frames within a control channel multiframe. The physical Frequency Correction Burst (FCB) is used to implement the logical FCCH.

11.4.3 GSM Traffic Channels

Voice channels are called Traffic Channels (TCH) in GSM. Traffic channels are two-way channels carrying the voice and data traffic between the MS and BTS. In the GSM standard, TCH data may not be sent in TS 0 within a TDMA frame on certain ARFCNs that serve as the broadcast station for each cell (since TS 0 is reserved for control channel bursts in every frame). Traffic channels carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link. One RF channel is shared by eight voice transmissions using TDMA. In terms of spectral efficiency, GSM works out to 25 kHz per voice channel, compared to about 30 kHz for AMPS and about 10 kHz for TDMA-based IS-54 or IS-136 systems. This is an approximate comparison as it ignores differences in control-channel overhead. As in TDMA-based systems, the mobile transmitter operates only during its allotted time slot. Assuming other parameters similar, a GSM mobile phone has longer battery life than a phone using either AMPS or IS-54/IS-136 because GSM mobile transmits in one-eighth of the time, compared with one-third of the time in TDMA-based IS-54/IS-136 system.

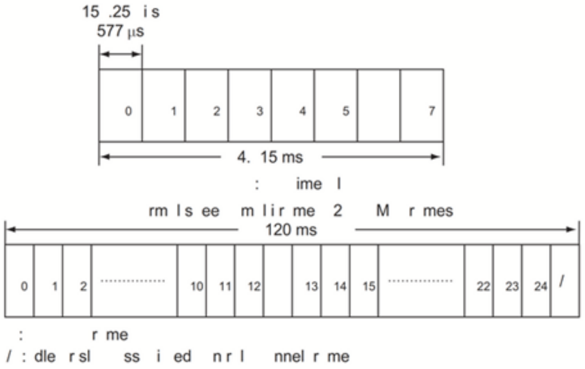


Fig. 11.12 *The TCH frame and multiframe structure*

Figure 11.12 illustrates how the TCH data is transmitted in consecutive frames.

Furthermore, frames of TCH data are broken up every thirteenth frame by either Slow Associated Control Channel Data (SACCH) or idle frames. Each group of twenty-six consecutive TDMA frames is called a multiframe (or speech multiframe, to distinguish it from the control channel multiframe described later). For every twenty-six frames, the thirteenth and twenty-sixth frames consist of Slow Associated Control Channel (SACCH) data, or the idle frame, respectively. The twenty-sixth frame contains idle bits for the case when full-rate TCHs are used, and contains SACCH data when half-rate TCHs are used. TCH logical channels are implemented over the normal burst. There are two types of TCH channels:

The full-rate traffic channel (TCH/F) uses a 13 kbps speech-coding scheme and 9,600 bps, 4,800 bps, and 2,400 bps data. After including signaling overhead, each full-rate traffic channel has a gross bit rate of 22.8 kbps for the network. When transmitted as full-rate, user data is contained within one time slot per frame. The following full-rate speech and data channels are supported:

Full-Rate Traffic Data Channel (TCH/F) The full-rate speech channel carries user speech that is digitised at a raw data rate of 13 kbps. With GSM channel coding added to the digitised speech, the full-rate speech channel carries 22.8 kbps.

Full-Rate Data Channel at 9600 bps (TCH/F9.6) The full-rate traffic data channel carries raw user data that is sent at 9600 bps. With additional forward-error-correction coding applied by the GSM standard, the 9600 bps data is sent at 22.8 kbps.

Full-Rate Data Channel at 4800 bps (TCH/F4.8) The full-rate traffic data channel carries raw user data that is sent at 4800 bps. With additional forward-error-correction coding applied by the GSM standard, the 4800 bps is sent at 22.8 kbps.

Full-Rate Data Channel at 2400 bps (TCH/F2.4) The full-rate traffic data channel carries raw user data that is sent at 2400 bps. With additional forward error correction coding applied by the GSM standard, the 2400 bps is sent at 22.8 kbps.

The half-rate traffic channel (TCH/H) uses 16 time slots per frame that has a gross bit rate of 11.4 kbps (half of gross bit rate of full-rate traffic channel). The half-rate TCH supports 4800 bps and 2400 bps data rate only. When transmitted as half-rate, user data is mapped onto the same time slot, but is sent in alternate frames. That is, two half-rate channel users would share the same time slot, but would alternately transmit during every other frame. The following half-rate speech and data channels are supported:

Half-Rate Traffic Data Channel (TCH/H) The half-rate speech channel has been designed to carry digitised speech which is sampled at a rate half that of the full-rate channel. GSM anticipates the availability of speech coders that can digitise speech at about 6.5 kbps. With GSM channel coding added to the digitised speech, the half-rate speech channel will carry 11.4 kbps.

Half-Rate Traffic Data Channel at 4800 bps (TCH/H4.8) The half-rate traffic data channel carries raw user data that is sent at 4800 bps. With additional forward-error-correction coding applied by the GSM standard, the 4800 bps data is sent at 11.4 kbps.

Half-Rate Traffic Data Channel at 2400 bps (TCH/H2.4) The half-rate traffic data channel carries raw user data that is sent at 2400 bps. With additional forward-error-correction coding applied by the GSM standard, the 2400 bps data is sent at 11.4 kbps.

The cell-site instructs the mobile subscriber to advance or retard the timing of its transmissions to compensate for the changes in propagation delay as it moves about in the cell. In this way, the transmission delay problem is avoided on the traffic channels.

7. a. Describe different identifiers used in GSM system. [7] CO5 L2

b. The GSM system uses the GMSK modulation scheme. Calculate the bandwidth efficiency of the standard GSM system. [3] CO5 L3

7.a.

11.3 IDENTIFIERS USED IN GSM SYSTEM

Several identity numbers are associated with a GSM system, which are briefly described below.

11.3.1 IMSI

The International Mobile Subscriber Identity (IMSI) number is usually 15 digits or less. When an MS attempts a call, it needs to contact a BS. The BS can offer its service only if it identifies the MS as a valid subscriber. For this, the MS needs to store certain values uniquely defined for the MS, like the country of subscription, network type, subscriber ID, and so on. These values are called the International Mobile Subscriber Identity (IMSI). The structure of an IMSI is shown in Fig. 11.5. The first three digits specify the country code, the next two specify the network provider code, and the rest are the mobile subscriber identification code (the customer ID number).

Another use of IMSI is to find information about the subscriber's home Public Land Mobile Network (PLMN). All such information is placed on the SIM card.

11.3.2 Subscriber Identity Module (SIM)

Every time the MS has to communicate with a BS, it must correctly identify itself. An MS does this by storing the mobile phone number, personal identification number for the mobile station, authentication parameters, and so on, in the SIM card. Smart SIM cards also have a flash memory that can be used to store small messages sent to the unit.

The main advantage of SIM is that it supports roaming with or without a cellphone, also called *SIM roaming*. All a user needs to do is to carry the SIM card alone, and insert it into any GSM mobile phone to make it work as per customised MS. In other words, the SIM card is the heart of a GSM mobile phone, and the MS hardware equipment is unusable without it.

11.3.3 Mobile System ISDN (MSISDN)

MSISDN is the number that identifies a particular MS's subscriber, with the format shown in Fig. 11.6.

The GSM actually does not identify a particular mobile phone, but a particular HLR. It is the responsibility of the HLR to contact the mobile phone.

11.3.4 Location Area Identity (LAI)

As shown in Fig. 11.7, the GSM service area is usually divided into a hierarchical structure that facilitates the system to access any MS quickly.

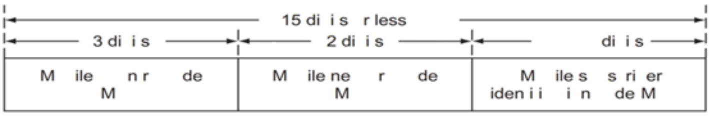


Fig. 11.5 Format of IMSI

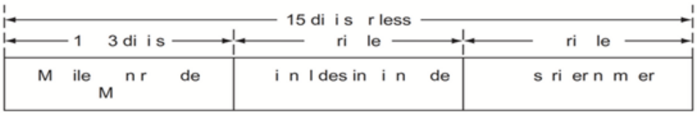


Fig. 11.6 Format of MSISDN

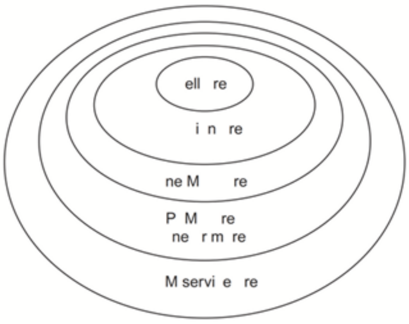


Fig. 11.7 GSM system hierarchy

Each PLMN area is divided into many MSCs. Each MSC typically contains a VLR to inform the system if a particular cellphone is roaming, and if it is roaming, the VLR of the MSC, in which the cellphone is, reflects the fact. Each MSC is divided into many Location Areas (LAs). An LA is a cell or a group of cells and is useful when the MS is roaming in a different cell but the same LA. Since any LA has to be identified as a part of the hierarchical structure, the identifier should contain the country code, the mobile network code, and the LA code.

11.3.5 IMSEI

Each manufactured GSM mobile phone equipment is assigned a 15-bit long International MS Equipment Identity (IMSEI) number to contain manufacturing information, as shown in Fig. 11.8. Conceptually, when the mobile phone equipment passes the interoperability tests, it is assigned a type approval code. Since a single mobile unit may not be manufactured at the same place, a field in IMSEI, called the final assembly code, identifies the final assembly place of the mobile unit. To identify uniquely a unit manufactured, a Serial Number (SN) is assigned. A spare digit is available to allow further assignment depending on requirements.

11.3.6 MS Roaming Number (MSRN)

When an MS roams into another MSC, that unit has to be identified based on the numbering scheme format used in that MSC. Hence, the MS is given a temporary roaming number called the MS Roaming Number (MSRN), with the format shown in Fig. 11.9. This MSRN is stored by the HLR, and any calls coming to that MS are rerouted to the cell where the MS is currently located.

11.3.7 TMSI

As all transmission is sent through the air interface, there is a constant threat to the security of information sent. A temporary identity Temporary Mobile Subscriber Identity (TMSI) is usually sent in place of IMSEI.

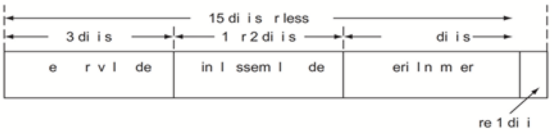


Fig. 11.8 | *Format of IMSEI*

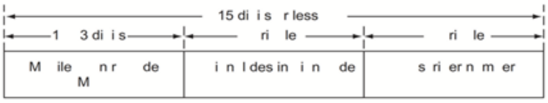


Fig. 11.9 | *Format of MSRN*

7.b.

Solution

$$\text{The channel bandwidth} = 200\text{ kHz} \qquad \text{(standard)}$$
$$\text{The channel data rate} = 270.833\text{ kbps} \qquad \text{(standard)}$$
$$\text{Bandwidth efficiency} = \text{Channel data rate/Channel bandwidth}$$

Therefore, $\text{bandwidth efficiency} = 270.833\text{ kbps}/200\text{ kHz}$

Hence, $\text{bandwidth efficiency} = 270.833\text{ kbps}/200\text{ kHz} = 1.35\text{ bps/Hz}$

8. What are the different protocols used in GSM signaling? Explain the protocol architecture in GSM signaling. [10] CO5 L2

11.2 GSM SIGNALING PROTOCOL ARCHITECTURE

Figure 11.2 shows the signaling protocol architecture for communication between the main hardware elements of the GSM network architecture and the associated interfaces.

The GSM standard specifies the interfaces among all the elements of the architecture. The air-interface 'U_m', which specifies communication between the MS and BTS, is the wireless related interface. Messages between the BTS and BSC flow through the A-bis interface. The support on this interface is for voice traffic at 64 kbps and data/signaling traffic at 16 kbps. Both types of traffic are carried over LAPD (which is a data link protocol used in ISDN).

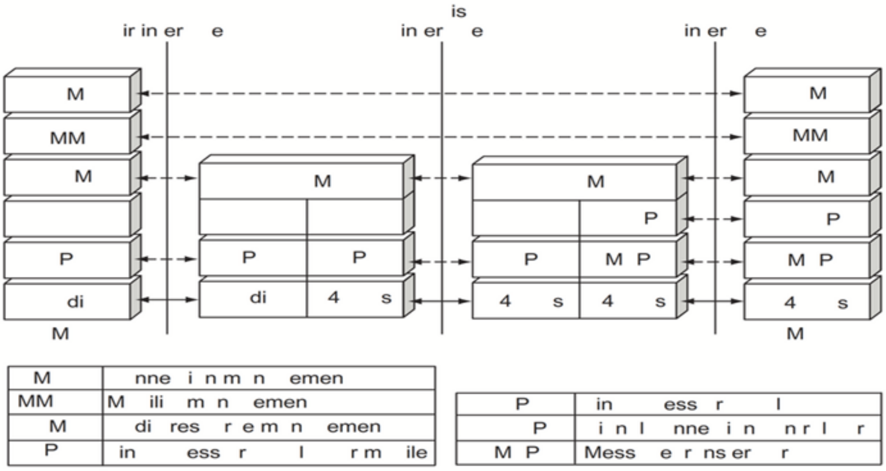


Fig. 11.2 | *The GSM signaling protocol architecture*

The interface between a BSC and a MSC is called the A' interface, which is standardised within GSM. The A' interface uses an SS7 protocol called the Signaling Connection Control Part (SCCP) which supports communication between the MSC and the BSS, as well as network messages between the individual mobile subscribers and the MSC. The A' interface allows a service provider to use base stations and switching equipment made by different manufacturers.

A number of control messages are exchanged between the key entities of GSM network architecture that deal with radio resources, mobility management, and connection management. The protocol stack is divided into three layers:

Layer 1 Physical Layer
Layer 2 Data Link Layer (DLL)
Layer 3 Networking or Messaging Layer

11.2.1 Layer I: Physical Layer

The physical layer defined in the GSM specifications is for the U_m air-interface. The radio link carries higher-level data inside the TDMA format between the mobile station and the base transceiver station. This layer specifies how the information from different voice and data services are formatted into packets and sent through the radio channel. It specifies the radio modem details, the packaging of a variety of services into the bits of a packet, traffic structure and control packets. This layer specifies modulation and coding techniques, power control methodology, and time synchronisation approaches which enable establishment and maintenance of the channels. The physical layer of the A and A-bis interfaces follow the ISDN standard with 64 kbps digital data per voice user.

11.2.2 Layer II: Data Link Layer

The control and signaling data transfer may be through the same physical channels or through separate physical channels. Signaling and control data are conveyed through Layer II and Layer III messages. At the link layer, a data link control protocol known as LAPD_m is used where *m* refers to the modified version of LAPD adapted to the mobile environment. In essence, LAPD is designed to convert a potentially unreliable physical link into a reliable data link. It does this by using a cyclic redundancy check to perform error detection and Automatic Repeat Request (ARQ) to retransmit damaged frames. The LAPD protocol is used for the A-bis and A interfaces connecting the BTS to BSC and BSC to MSC, respectively.

The overall purpose of DLL is to check the flow of packets for Layer III and allow multiple Service Access Points (SAP) with one physical layer. The remaining links use the normal LAPD protocol. The DLL checks the address and sequence number for Layer III and manages acknowledgments for transmission of the packets. In addition, the DLL allows two SAPs for signaling and Short Messages (SMS). The SMS traffic channel in the GSM is not communicated through voice channels. In GSM, the SMS is transmitted through a fake signaling packet that carries user information over signaling channels. The DLL in GSM provides this mechanism for multiplexing the SMS data into signaling streams.

Signaling packets delivered to the physical layer are each 184 bits, same as that of the length of the DLL packets in the LAPD protocol used in the ISDN networks. The length of the LAPD_m packets, shown in Fig. 11.3, is the same as LAPD, but the format is slightly adjusted to fit the mobile environment.

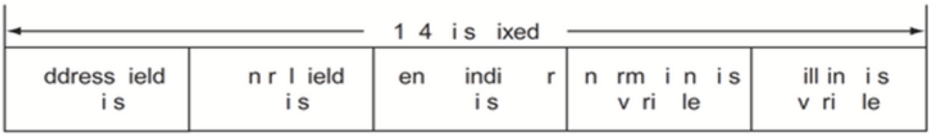


Fig. 11.3 *Frame format of the Layer II in LAPD_m*

Since GSM has the time synchronisation and strong coding at the physical layer, the synchronisation bits and CRC codes in LAPD are eliminated in the LAPD_m. The address field is optional, and it identifies the SAP, protocol revision type, and nature of the message. The control field is also optional, and it holds the type of the frame (command or response) and the transmitted and received sequence numbers.

The length indicator identifies the length of the information field. Fill-in bits are all 1s bits to extend the length to the desired 184 bits. In peer-to-peer Layer II communications, such as DLL acknowledgments, there is no Layer III payload and fill-in bits cover this field. The information field carries the Layer III payload data.

The peer-to-peer Layer II messages are *unnumbered acknowledgment, receiver ready, receiver not ready, disconnect*, and *reject*. These messages do not have Layer III information bits and are referred to as Layer II messages. The information bits in Layer II packets specify Layer III operations implemented on the logical signaling channels. These information bits are different for different operations.

11.2.3 Layer III: Networking or Signaling Layer

The networking or signaling layer implements the protocols needed to support the mechanisms required to establish, maintain, and terminate a mobile communication session. It is also responsible for control functions for supplementary and SMS services. The traffic channels are carried by normal bursts in different formats associated with different speech or data services. The signaling information uses other bursts and more complicated DLL packaging. A signaling procedure such as the registration process is composed of a sequence of communication events or messages between hardware elements of the systems that are implemented on the logical channels encapsulated in the DLL frames.

Layer III defines the details of implementation of messages on the logical channels encapsulated in DLL frames. Among all messages communicated between two elements of the network only a few, such as DLL acknowledgment, do not carry Layer III information. Information bits of the Layer II packets specify the operation of a Layer III message. As shown in Fig. 11.4, these bits are further divided into several fields.

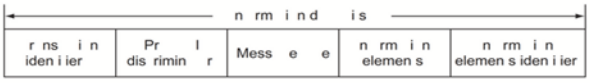


Fig. 11.4 | *Typical Layer III message format*

The Transaction Identifier (TI) field is used to identify a procedure or protocol that consists of a sequence of messages. This field allows multiple procedures to operate in parallel. The Protocol Discriminator (PD) identifies the category of the operation (management, supplementary services, call control, and test procedure). The Message Type (MT) identifies the type of message for a given PD. Information Elements (IE) is an optional field for the time that an instruction carries some information that is specified by an IE Identifier (IEI). The number of Layer III messages is much larger than the number of Layer II messages.

To further simplify the description of the Layer III messages, GSM standard divides the messages into three sublayers that provide specific functions:

- Radio Resource Management (RRM)
- Mobility Management (MM)
- Communication Management (CM)

The RRM sublayer of Layer III manages the frequency of operation and the quality of the radio link. Radio resource management establishes and releases connections between MSs and an MSC and maintains them despite subscriber movements. The RRM functions are mainly performed by the MS and the BSC. The main responsibilities of the RRM are to assign the radio channel and hop to new channels in implementation of the slow frequency-hopping option, to manage hand-off procedure and measurement reports from MS for hand-off decision, to implement power control procedure, and to adapt to timing advance for synchronisation.

The major functions of Mobility Management (MM) sublayer are location update, registration procedures, authentication procedure, TMSI handling, and attachment and detachment procedures for the IMSI. This sublayer handles mobility issues that are not directly related to the radio, and include management of security functions. Mobility management functions are handled by the MS/SIM, the MSC/VLR, and the HLR/AuC.

The Communication Management (CM) sublayer is used to establish, maintain, and release the circuit-switched connection between the calling and called subscribers of GSM network. Specific procedures for the CM sublayer include mobile-originated and mobile-terminated call establishment, change of transmission mode during the call, control of dialing using dual-tones, and call reestablishment. In addition to call management, it includes supplementary services management and SMS management.

The Mobile Application Part (MAP) handles most of the signaling between different entities in the fixed part of the network, such as between the HLR and VLR. It runs on top of two intermediate protocols—Signal Connection Control Part (SCCP) and Message Transfer Part (MTP). SCCP and MTP protocols are part of Signaling System Number 7, which is a set of protocols designed to provide control signaling within digital circuit-switching networks.

Facts to Know!

SS7 is also used for many other Intelligent Network Services (like virtual calling card service and local number portability) within the GSM.

11.2.4 SS7 Signaling

Common Channel Signaling System No. 7 (SS7 or CC7) is a global standard that defines the procedures and protocol by which network elements in PSTN exchange information over a digital signaling network to effect wireless (cellular) and wireline call set-up, routing and control. The SS7 signaling protocols are mainly used for basic call set-up, call management, wireless services such as PCS, wireless roaming, mobile subscriber authentication, local number portability, toll-free and toll wireline services, enhanced call features such as call forwarding, calling party name/number display, and three-way calling, efficient and secure worldwide telecommunications. The SS7 protocol provides both error correction and retransmission capabilities to allow continued service in the event of signaling point or link failures.

SS7 messages are exchanged between network elements over 64 kbps bi-directional channels called signaling links. Signaling occurs out-of-band on dedicated channels rather than in-band on voice channels. Compared to in-band signaling, out-of-band signaling provides faster call set-up times, more efficient use of voice circuits, support for Intelligent Network (IN) services which require signaling to network elements without voice trunks (for example, database systems), and improved control over fraudulent network usage. There are three kinds of signaling points in the SS7 network:

- Service Switching Point (SSP)
- Signal Transfer Point (STP)
- Service Control Point (SCP)

SSPs are switches that originate, terminate, or tandem calls. An SSP sends signaling messages to other SSPs to set up, manage, and release voice circuits required to complete a call. An SSP may also send a query message to a centralised database, an SCP, to determine how to route a call. An SCP sends a response to the originating SSP containing the routing number(s) associated with the dialed number. An alternate routing number may be used by the SSP if the primary number is busy or the call is unanswered within a specified time. Actual call features vary from network to network and from service to service.

Network traffic between signaling points may be routed via a packet switch called STP. The STP routes each incoming message to an outgoing signaling link based on routing information contained in the SS7 message. Because it acts as a network hub, STP provides improved utilisation of the SS7 network by eliminating the need for direct links between signaling points. The STP may perform global title translation, a procedure by which the destination signaling point is determined from digits present in the signaling message. The STP can also act as a firewall to screen SS7 messages exchanged with other networks. Because the SS7 network is critical to call processing, SCPs and STPs are usually deployed in pair configurations in separate physical locations to ensure network-wide service in the event of an isolated failure.

Facts to Know!

SCPs provide the access mechanism required for a service. These are used for a variety of applications such as calling card verification, toll-free calls, and premium tariff calls.

11.2.5 Addressing and Routing

Within the GSM network, two types of routing can be described:

- SS7 addressing and message signaling routing
- Call control/number routing

The SS7 MTP layer 3 provides the routing function. This layer is used to route within a local network using the Signaling Point Code addressing. To interconnect all the local networks on the national SS7 networks, the SCCP Global Title Translation (GTT) functionality is used. Global Title Translation is one of the strong routing capabilities of SS7 SCCP layer. This SCCP functionality allows a centralised network to hold and maintain all the addresses and routing tables, centralising the routing function. For MSC to send a message to a particular HLR, the MSC does not need to know each Mobile's HLR point code. Only the adjacent STP point code and the dialed digits (MSISDN) needs to be provided to the STP in order to route the message to the HLR. The STP will perform the translation of the dialed digits to physical point code (HLR or MSC).

The STP pair after checking the SCCP header information will determine if the message requires GTT translation. It will then extract the IMSI of the subscriber from the calling number address field in the SCCP header

Facts to Know!

STP is similar to a switch or a node in the SS7 signaling network performing the basic routing functions. For fault tolerance, STPs are always installed in pairs with cross-connections.

and from a database table determine the HLR point code where the validation/authentication should be sent. This will eliminate book-keeping on every MSC and centralise the routing/translation on the SS7 STP network.

A landline calling party dials the GSM mobile directory number (MS ISDN number). The PSTN after performing the digits translation routes the call to the home PLMN GMSC. The GMSC contains either the routing tables to relate the MSISDN number with the corresponding HLR, or if the GMSC is connected to the SS7 network with the GTT functionality, the SS7 network will identify the HLR. Once the GMSC interrogates the HLR with the MSISDN number, the HLR determines the IMSI from the MSISDN number. The HLR stores the subscriber's information based on IMSI, not MSISDN. The HLR locates the visiting MSC/VLR point code and if the MSRN is available, it will return the information to GMSC. If the HLR does not have the MSRN for the subscriber it will request one from the visiting MSC/VLR. The latter can be done via GTT if an SS7 backbone with GTT (IMSI to point code) functionality is available/supported. The GMSC once it receives the MSRN and the MSC/VLR point code, will route the call to the VMSC/VLR. The MSC/VLR will then page the mobile subscriber.

The call-originating information including the dialed digits will be sent to the MSC/VLR. The MSC/VLR with the subscriber's profile information performs digits translation (if supported) and routes the call either to the PSTN or to other MSCs. If the MSC cannot perform the digits translation it would route the call to GMSC for translation and routing.

11.2.6 Location Update

A list of relevant functions of a mobile station includes provision of location updates. The location-updating procedures, and subsequent call routing, use the MSC and two location registers: HLR and VLR. When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location. In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number.

Facts to Know!

The reason a routing number is not normally assigned, even though it would reduce signaling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls.

If the subscriber is entitled to service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration. For reliability reasons, the GSM also has a periodic location updating procedure. If an HLR or MSC/VLR fails, to have each mobile register simultaneously to make the database up-to-date would cause overloading. Therefore, the database is updated as location updating events occur. The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signaling traffic and speed of recovery. If a mobile does not register after the updating time period, it is de-registered.

A procedure related to location updating is the IMSI attach and detach. A detach permits the network to know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages. An attach is similar to a location update, and informs the system that the mobile is reachable again. The activation of IMSI attach/detach is up to the operator on an individual cell basis. Location update is a typical example for the connection-oriented transactions in GSM. The local operation code UpdatLocation is required directly after the location update for the new VLR to update the location information in the HLR. Because this is a confirmed service, it requires all four variants: request, indication, response and confirmation.