CMR Institute of Technology
Department of ECE
18EC81-Wireless and Cellular communication
Assignment-2

S.no	Questions	Bloom's Level
1.	Explain the following interfaces of GSM a) Um interface b) Abis interface c) A interface A series of different interface definitions were written and each given names as seen below. • ***Um interface*** The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signalling, a modified version of the ISDN LAPD, known as LAPDm is used. • ***Abis interface*** This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardised. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS. • ***A interface*** The A interface is used to provide communication between the BSS and the MSC. The interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipments being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface. • ***B interface*** The B interface exists between the MSC and the VLR . It uses a protocol known as the MAP/B protocol. As most VLRs are collocated with an MSC, this makes the interface purely an "internal" interface. The interface is used whenever the MSC needs access to data regarding a MS located in its area. • ***C interface*** The C interface is located between the HLR and a GMSC or a SMS-G. When a call originates from outside the network, i.e. from the PSTN or another mobile network it ahs to pass through the gateway so that routing information required to complete the call may be gained. The protocol used for communication is MAP/C, the letter "C" indicating that the protocol is used for the "C" interface. In addition to this, the MSC may optionally forward billing information to the HLR after the call is completed and cleared down. • ***D interface*** The D interface is situated between the VLR and HLR. It uses the MAP/D protocol to exchange the data related to the location of the ME and to the management of the subscriber. • ***E interface*** The E interface provides communication between two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol. • ***F interface*** The F interface is used between an MSC and EIR. It uses the MAP/F protocol. The communications along this interface are used to confirm the status of the IMEI of the ME gaining access to the network. • ***G interface*** The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure. • ***H interface*** The H interface exists between the MSC the SMS-G. It transfers short messages and uses the MAP/H protocol. • ***I interface*** The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through	L2

	the BSS. In some cases the 2G GSM interfaces were not as rigorously defined as many might have liked, but the did at least provide a large element of the definition required, enabling the functionality of GSM network elements to be defined sufficiently. Note: Usually a) Um interface b) Abis interface c) A interface are asked.	
2.	Describe the GSM frame structure. • Each user transmits a burst of data during the time slot assigned to it. These data bursts may have one of five specific formats. Normal bursts are used for TCH and DCCH transmissions on both the forward and reverse link. FCCH and SCH bursts are used in TS0 of specific frames to broadcast the frequency and time synchronization control messages on the forward link. The RACH burst is used by all mobiles to access service from any base station, and the dummy burst is used as filler information for unused time slots on the forward link. • A frame is one where no time slot is repeated. A frame contains eight time slots TS0 to TS7. One time slot duration= 576.92 μsec576.92 μsec Number of bits transmitted during 1 time slot= 156.25 bits Thus duration of one frame = 576.92μsec×8=4.6153 msec576.92μsec×8=4.6153 msec Each bit duration = 576.92 μsec156.25 bits=3.6922 μsec576.92 μsec156.25 bits=3.6922 μsec Transmission rate = 156.25 bits576.92 μsec=270.833 kbps156.25 bits576.92 μsec=270.833 kbps One user's transmission rate = 270.833 kbps / 8 = 33.854 kbps • One single time slot in frame has eight fields as follows: ○ **Tale bits:** They are present at the start and end of every time slot to distinguish one time slot from another. It identifies beginning and end of the burst. ○ **Coded data:** This is the actual information to be transmitted. Out of 156.25 bits 114 are information bearing bits that are transmitted as two 57 bits sequences close to beginning and end of the time slot. ○ **Stealing flag:** This bit helps base station to distinguish whether the coded data is control or actual information.	L2

At the time of urgency control its are also sent using voice channel at that time stealing bit becomes '0' indicating coded data carries control information.

- **Midamble:** This consists of 26 bits training sequence. It helps the adaptive equalizer in mobile or base station receiver to analyze radio channel characteristics before coding. It gives the amount of fading the channel provides helping to decide which equalizer to be used.
- **Guard period:** A guard time of 8.25 bits is provided at the end of every time slot to prevent overlapping with next time slot preventing actual information from getting tampered.

- During a frame a GSM subscriber uses on one time slot to transmit and one time slot to receive and may use spare five time slots to measure signal strength on adjacent five base station as well as its own base station.

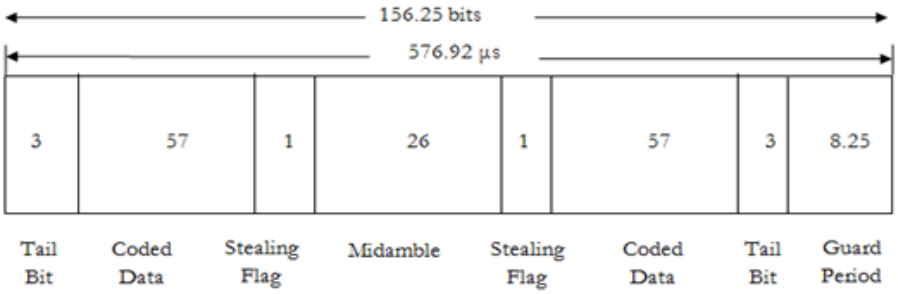


Fig: One time slot structure

- Each normal speech frames are grouped into larger structures called Multiframes which in turn are grouped into superframes and hyperframes.

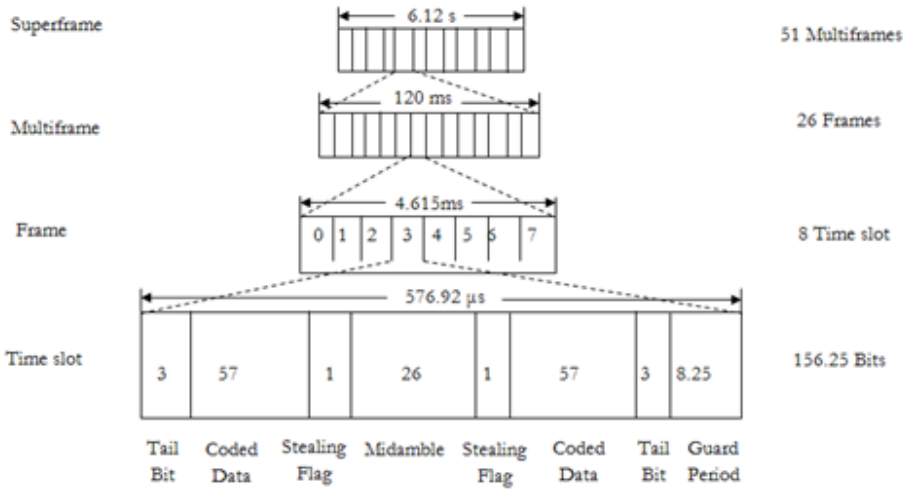


Fig: Frame Hierarchy

- One Multiframe contains 26 TDMA frames, one superframe contains 51 multiframes or 1326 TDMA frames and one hyperframe contains 2048 superframes or 2715648 TDMA frames. One hyperframe is transmitted after every 3.4815 hours.
- Hyperframe is important in GSM because the encryption algorithms rely on particular frame number and sufficient security can only be obtained by using a large number of frames as provided by hyperframe.

3.	Draw the block diagram explaining the architecture of GSM involving four subsystems and explain each in detail. The GSM architecture consists of three major interconnected subsystems that interact with themselves and with users through certain network interface. The subsystems are Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operational Support Subsystem (OSS). Mobile Station (MS) is also a subsystem but it is considered as a part of BSS. **1. Mobile Station (MS):** Mobile Station is made up of two entities. **A. Mobile equipment (ME):** • It is a portable, vehicle mounted, hand held device. • It is uniquely identified by an IMEI number. • It is used for voice and data transmission. It also monitors power and signal quality of surrounding cells foe optimum handover. 160 characters long SMS can also be sent using Mobile Equipment.	L2

B. Subscriber Identity module (SIM):

- It is a smart card that contains the International Mobile Subscriber Identity (IMSI) number.
- It allows users to send and receive calls and receive other subscriber services. - It is protected by password or PIN.
- It contains encoded network identification details. it has key information to activate the phone.
- It can be moved from one mobile to another.

2. Base Station Subsystem (BSS): It is also known as radio subsystem, provides and manages radio transmission paths between the mobile station and the Mobile Switching Centre (MSC). BSS also manages interface between the mobile station and all other subsystems of GSM. It consists of two parts.

A. Base Transceiver Station (BTS):

- It encodes, encrypts, multiplexes, modulates and feeds the RF signal to the antenna.
- It consists of transceiver units.
- It communicates with mobile stations via radio air interface and also communicates with BSC via Abis interface.

B. Base Station Controller (BSC):

- It manages radio resources for BTS. It assigns frequency and time slots for all mobile stations in its area.
- It handles call set up, transcoding and adaptation functionality handover for each MS radio power control.
- It communicates with MSC via A interface and also with BTS.

3. Network Switching Subsystem (NSS): it manages the switching functions of the system and allows MSCs to communicate with other networks such as PSTN and ISDN. It consist of

A. Mobile switching Centre:

- It is a heart of the network. It manages communication between GSM and other networks.
- It manages call set up function, routing and basic switching.
- It performs mobility management including registration, location updating and inter BSS and inter MSC call handoff.
- It provides billing information.
- MSC does gateway function while its customers roam to other network by using HLR/VLR.

B. Home Location Registers (HLR): - It is a permanent database about mobile subscriber in a large service area. - Its database

	contains IMSI, IMSISDN, prepaid/post-paid, roaming restrictions, supplementary services. **C. Visitor Location Registers (VLR):** - It is a temporary database which updates whenever new MS enters its area by HLR database. - It controls mobiles roaming in its area. It reduces number of queries to HLR. - Its database contains IMSI, TMSI, IMSISDN, MSRN, location, area authentication key. **D. Authentication Centre:** - It provides protection against intruders in air interface. - It maintains authentication keys and algorithms and provides security triplets (RAND, SRES, Ki). **E. Equipment Identity Registry (EIR):** • It is a database that is used to track handset using the IMEI number. • It is made up of three sub classes- the white list, the black list and the gray list. **4. Operational Support Subsystem (OSS):** It supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose and troubleshoot all aspects of GSM system. It supports one or more Operation Maintenance Centres (OMC) which are used to monitor the performance of each MS, Bs, BSC and MSC within a GSM system. It has three main functions: • To maintain all telecommunication hardware and network operations with a particular market. • To manage all charging and billing procedures • To manage all mobile equipment in the system. **Interfaces used for GSM network : (ref fig 2)** 1)UM Interface –Used to communicate between BTS with MS 2)Abis Interface— Used to communicate BSC TO BTS 3)A Interface-- Used to communicate BSC and MSC 4) Singling protocol (SS 7)- Used to communicate MSC with other network .	

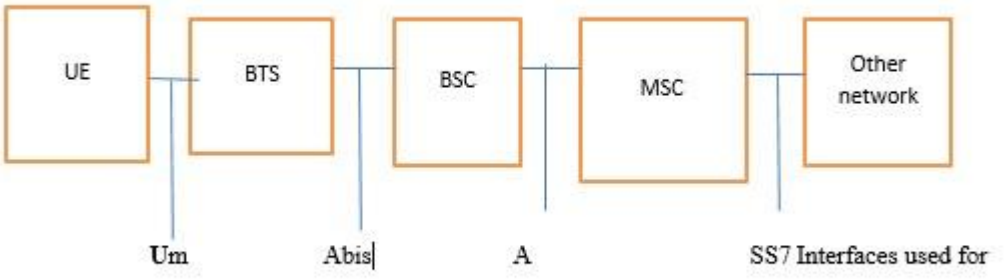


Fig 2 GSM network Interfaces

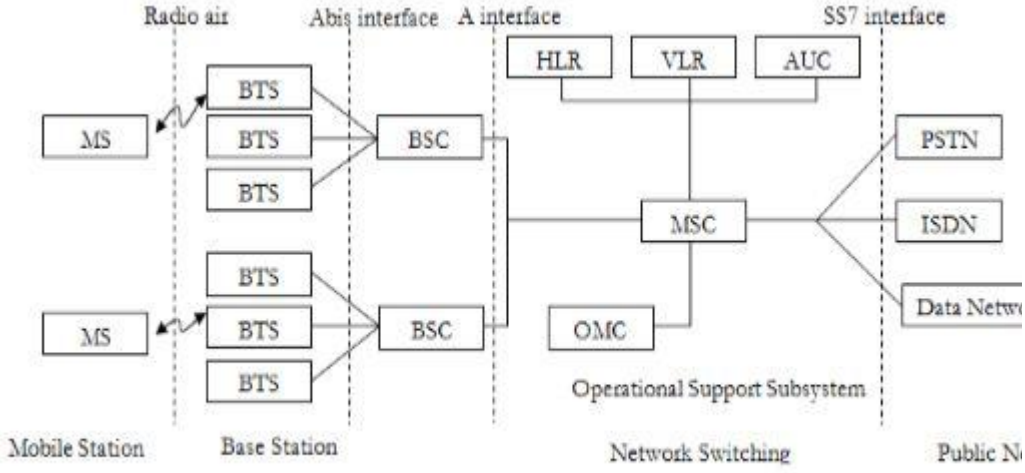
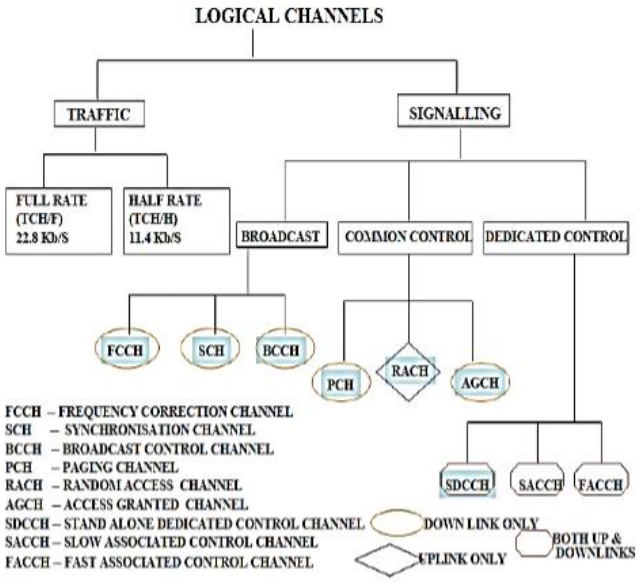


Fig: GSM Architecture

4.	Discuss the classification of GSM channels in detail. GSM Channel are divided into two types: **Traffic channels (TCHs):** • The traffic channes are intended to carry encoded speech or user data. • Traffic channels are intended to carry encoded speech and user data. • Full rate traffic channels at a net bit rate of 22.8 Kb/s (TCH/F) • Half rate traffic channels at a net bit rate of 11.4 Kb/s (TCH/H) • Speech channels are defined for both full rate and half rate traffic channels. • Data channels support a variety of data rates (2.4, 4.8 and 9.6 Kb/s) on both half and full rate traffic channels. The 9.6 Kb/s data rate is only for full rate application.	L2



- The traffic channels(TCH) support two types of information rates Full rate (TCH/F) and Half rate (TCH/H)
- When transmitted as full rate, the user data is occupied within TS per frame. When transmitted as half rate, the user data is occupied into the same time slot but sent in alternate frames.
- The 26th frame contains idle bits if full rate TCHs are used and contains SACCH data if half rate TCHS are used

- Full Rate TCH for data and speech channels:-

A. **Full - rate Speech Channel)TCH/Fs):** At 16 kbps the full rate speech channel is digitized. The full rate speech channel caries 55.8kbps after adding the GSM channel coding to the digitized speech.

B. **Full-rate Data Channel for 9600 bps (TCH/F9.6):** The full rate traffic data channel contains raw data that is transmitted at 9.6 kbps. After the application of additional forward error correction coding with the GSM standards, 9600 kbps is transferred at 22.8 kbps.

C. **Full-rate Data Channel for 4500 bps(TCH/F4.8):** The full rate traffic date channel contains data that is transmitted at 4.8 Kbps. After the application of additional forward error correction coding with GSM standards, the 4.8 kbps is transferred at 22.8 kbps.

D. **Full Rate Data Channel for 2400 bps (TCH/F2.4):** The full rate traffic data channel contains raw data that is transmitted at 2.4 kbps. After the application of additional forward error

correction coding with GSM standards, the 2.4 kbps data is transferred at 22.8 kbps.

. **Half Rate TCH for data and speech channels:**

A. **Half Rate Speech Channels (TCH/HS):** The half tate speech channel can carry digitized speech that is sampled at a rate half that of full rate channel. GSM anticipates the availibility of speech coders. It can digitize speech at about 6.5 kbps. After adding GSM channel coding to the digitized speech, the half rate Speech channel will carry 11.4 kbps.

B. **Half Rate Data Channel for 4800 bps (TCH/H4.8):** The half rate traffic data channel carries raw data that is sentat 4800 bps. After the application of forward error correction using GSM standards, 4800 bps data is sent at 11.4 kbps.

C **Half Rate Data Channe for 2400 kbps (TCH/H 2.4):** The half rate traffic data channel carries raw user data that is sent at 2400 bps. After application of additional forward error corretion using GSM standards, 2400 bps data is sent to 11.4 bps.

Control Channel (CCH):

. Control channels carry signaling information between an MS and a BTS.

a) **Broadcast control channel:**

. Broadcast control channels are transmitted in downlink direction only i.e. only transmitted by BTS.

. The broadcast channels are used to broadcast synchronization and general network information to all the MSs within a cell.

. **It has three types:**

a. **FREQUENCY CORRECTION CHANNEL (FCCH):**

. Used for the frequency correction / synchronization of a mobile station.

. The repeated (every 10 sec) transmission of Frequency Bursts is called FCCH.

b. **SYNCHRONISATION CHANNEL (SCH):**

. Allows the mobile station to synchronize time wise with the BTS.

. Repeated broadcast (every 10 frames) of Synchronization Bursts is called (SCH).

c. **BROADCAST CONTROL CHANNEL (BCH):**

. The BROADCAST CONTROL CHANNEL (BCCH) is used to

broadcast control information to every MS within a cell.

. This information includes details of the control channel configuration used at the BTS, a list of the BCCH carrier frequencies used at the neighboring BTSs and a number of parameters that are used by the MS when accessing the BTS.

Common Control Channel:

The common control channels are used by an MS during the paging and access procedures. Common control channels are of three types.

(PCH) PAGING CHANNEL:

. Within certain time intervals the MS will listen to the Paging channel, PCH, to see if the network wants to get in contact with the MS.

. The reason could be an incoming call or an incoming Short Message.

2.**(RACH) RANDOM ACCESS CHANNEL:**

- If listening to the PCH, the MS will realize it is being paged.
- The MS answers, requesting a signalling channel, on the Random Access channel, RACH.
- RACH can also be used if the MS wants to get in contact with the network, e/g. when setting up a mobile originated call.

3.**(AGCH) ACCESS GRANTED CHANNEL:**

- The access grant channel (AGCH) is carried data which instructs the mobile to operate in a particular physical channel (Time slot or ARFCN).
- It uses normal burst.

C) Dedicated Control Channels (DCCHs):

- Signaling information is carried between an MS and a BTS using associated and dedicated control channels during or not during a call, They are of three types:

A. (SDCCH STAND ALONE DEDICATED CONTROL CHANNEL:

- Non-urgent information, e.g. transmitter power control, is transmitted using the slow associated control channel (SACCH).
- On the uplink MS sends averaged measurements on own base station (signal strength and quality) and neighboring base stations (signal strength).
- On the downlink the MS receives system information, which

	transmitting power and what timing advance to use. It is transmitted at 13thFrame of TCH. As seen, SACCH is transmitted on both up-and downlink, point-to-point. • It uses normal burst. **B. (SAACH)SLOW ASSOCIATED CONTROL CHANNEL:** • In some situations, signaling information must flow between a network and an MS when a call is not in progress, e.g. during a location update. • This could be accommodated by allocating either a full-rate or half-rate TCH and by using either the SACCH or FACCH to carry the information. **C. (FACCH) FAST ASSOCIATED CONTROL CHANNEL:** • More urgent information, e.g. a handover command, is sent using time slots that are 'stolen' from the traffic channel. • If, suddenly, during the conversation a handover must be performed the Fast Associated Control channel, FACCH, is used. • FACCH works in stealing mode, meaning that one 2. ms segment of speech is exchanged for signaling information necessary for the handover.	
5.	Explain mapping of logical channel to physical in GSM. LTE defines two types of channels, logical channels and Physical channels. Logical channels are defined by the type of information that they carry and that are mapped to transport channels and from there to physical channels. Physical channels are defined by their physical properties, i.e., time, subcarrier etc. **1) Logical Channels:** The logical channels are similar to those in WCDMA, they are of two types, Traffic channels, Control Channels. Their functions are described as follows: • **Traffic channels** **a) Dedicated Traffic CHannel (DTCH):** It is a dedicated traffic channel to one user that carries the user data for all ULs, as well as for those downlink data that are not multicast/broadcast. **b) Multicast Traffic CHannel (MTCH):** It is a point to multipoint traffic channel that carries the user data for multicast/broadcast downlink transmission.	

- **Control channels**

  a) Broadcast Control CHannel (BCCH): It is a downlink channel that carries system information data that are broadcasted to the MSs in a cell. Note the difference from the MTCH, which also broadcasts to MSs, but carries user data.

  b) Paging Control CHannel (PCCH): It is a downlink channel that transfers paging information and system information change notifications to MSs in multiple cells. Specifically it is used when it is not known exactly in which cell the MS currently is located.

  c) Common Control CHannel (CCCH): It transmits control data for the Random Access (RA), i.e., when a connection is started.

  d) Dedicated Control CHannel (DCCH): It is used for the transmission of control information that relates to a specific MS (as opposed to the system information relevant for all MSs, which is broadcast in the BCCH).

  e) Multicast Control CHannel (MCCH): It carries the control information related to multicast/broadcast services.

2) Transport Channels:

The Logical channels are mapped onto the transport channels as illustrated in Figure 8: They are as follows:

a)Broadcast CHannel (BCH): It transmits a part of the BCCH (the remainder is on the DL- SCH described below)in the entire coverage area of the cell. It has a fixed predefined transport format, so that any MS can listen to it easily.

b) Paging CHannel (PCH): It transmits the PCCH in the entire coverage area of the cell, It supports discontinuous reception for power saving of MS/UE. It is mapped to physical resources which can also be used for traffic /other control channels.

c) Multicast Channel (MCH): It is used to support broadcast/multicast transmission in the entire coverage area of the cell. It has a semi static scheduling and transport format.

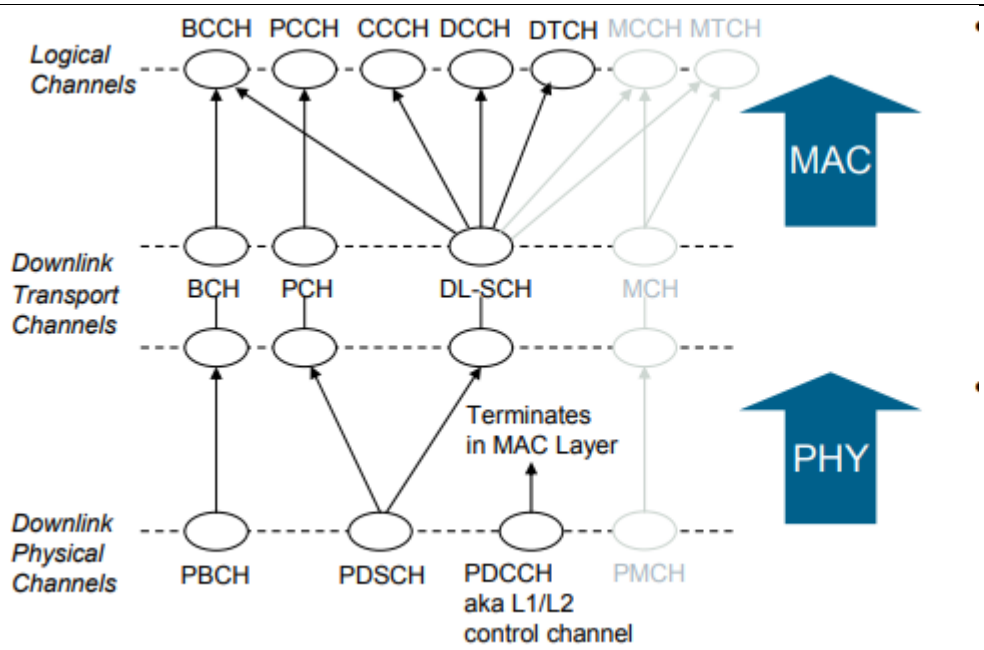


Figure 8: Illustration of mapping of logical channels to Transport channels

- **d) Down Link Shared Channel (DL- SCH) and Up Link Shared Channel (UL- SCH):** They carry the user data, as well as most of the control information (except the one already mentioned above).Theses channels also support Hybrid ARQ, dynamic link adaptation by varying the modulation, coding and transmit power. They also support dynamic and semi-static resource allocation and discontinuous reception to enable power saving of UE/MS. Optionally they can be used for beam forming and broadcasting in the entire coverage area. The data on transport channels are organized into transport blocks; in each transmission time interval (usually a sub frame = 2 time slots), one transport block is transmitted. A transport format is associated with each transport block. Finally, these transport channels are mapped onto physical channels; there are also physical channels that do not carry any transport channel, but are purely used for PHY functionality.

3) Physical Channels:

Transport channels are mapped into physical channels to carry user and control data. In this section the function of both downlink as well as uplink physical channels are presented.

- **Downlink Physical Channels**

  a) Physical Broadcast CHannel (PBCH): It carries the BCH. The coded BCH transport blocks are mapped to four sub

frames within a 40 ms interval. 40 ms timing is blindly detected i.e. there is no explicit signaling for indicating 40 ms timing. Each subframe is assumed to be self decodable i.e. BCH can be decoded in a single reception assuming good channel conditions. It supports QPSK modulation.

b) Physical Downlink Shared CHannel (PDSCH): It carries the DL-SCH, i.e., user data, some control data for the downlink, as well as the PCH. It supports QPSK,16 QAM and 64 QAM modulation formats.

c) Physical Multicast CHannel (PMCH): it carries the MCH, which contains the multicast payload, as well as some of the control information for multicast. It supports QPSK, 16 QAM and 64 QAM modulation formats.

d) Physical Downlink Control CHannel (PDCCH): It carries control information, such as scheduling that is required for reception of the PDSCH. This channel does not carry any transport channel.

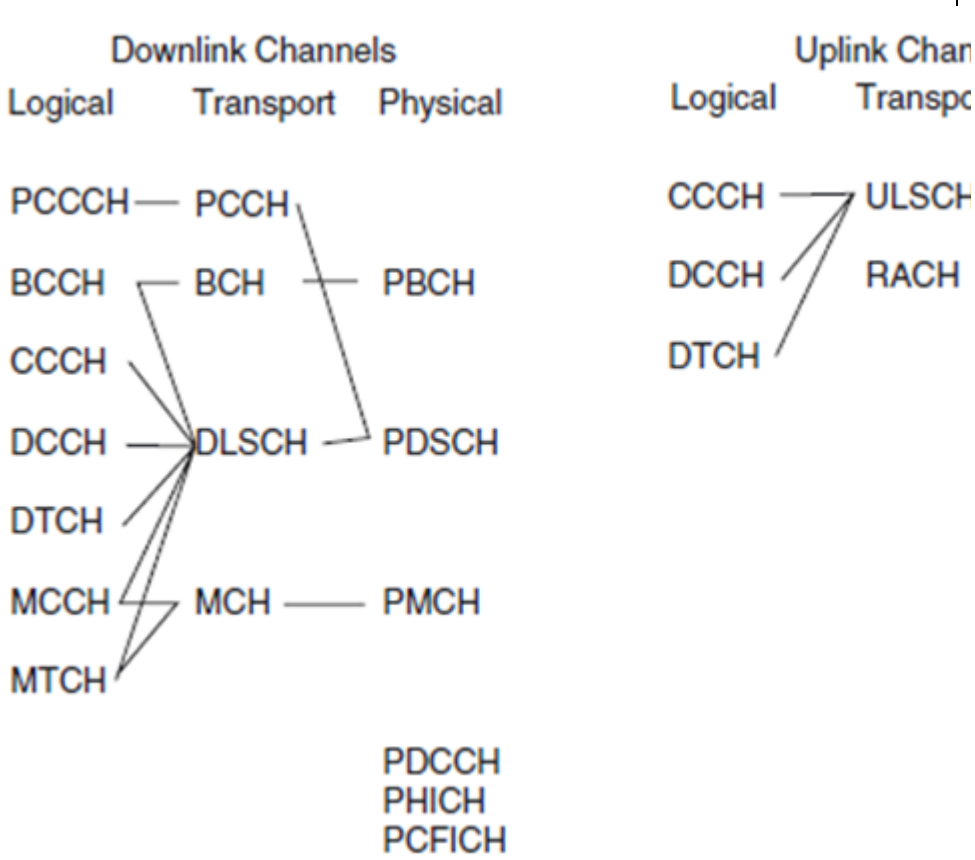
e) Physical Control Format Indicator CHannel (PCFICH): It carries control information about the PDCCH. This channel does not carry any transport channel.

f) Physical HARQ Indicator CHannel (PHICH): It carries the feedback bits indicating whether a retransmission of transport blocks is necessary. This channel does not carry any transport channel.

g) Synchronization Signal (SS): The SS carries information about the timing of the cell, as well as the cell ID. LTE actually provides two SSs, the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS). In contrast to other systems, these signals are not called “channels,” but perform similar functions as, e.g., the synchronization channels in WCDMA. To understand the functionality of the SS, keep in mind that there are 504 cell IDs defined for LTE, which are divided into 168 ID groups. The PSS is transmitted in the last symbol of the first slot of subframes 0 and 5 of every frame, extending over 72 subcarriers. The SSS signal is transmitted in the symbol directly before every PSS signal. The SSS carries information about the cell ID group: the signal also extends over 72 subcarriers.

- **Uplink Physical Channels**

  a) Physical Uplink Shared Channel (PUSCH): It is the uplink counterpart to the PDSCH.

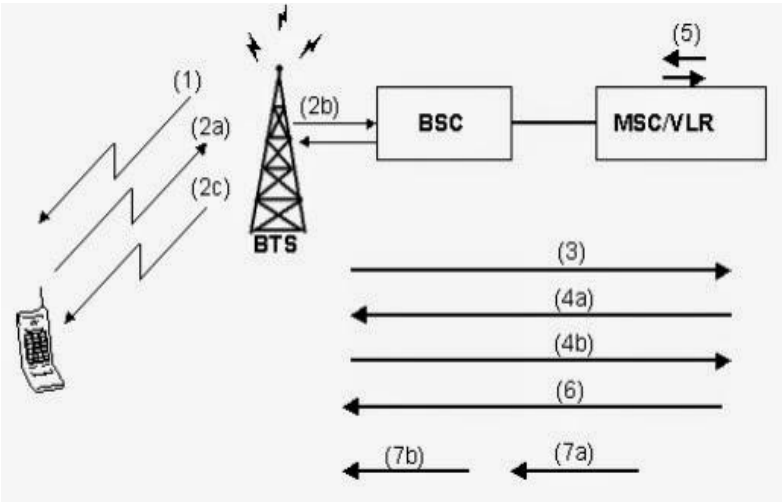
	b) Physical Uplink Control Channel (PUCCH): It carries mainly three types of information: (i) channel state feedback; (ii) resource requests (remember that the BS performs the scheduling, i.e., assigns all the resources also for the up link; thus the MS must request resources when it has data to transmit), and (iii) HARQ feedback bits. **c) Physical Random Access CHannel (PRACH):** it is used for the random access, i.e., MS communicating to the BS before a connection with scheduling has been established. Complete mapping of Logical to Transport to Physical channels for both downlink and uplink is illustrated in Figure 9.  **Figure 9: Mapping between Logical, Transport, and Physical channels**	
6.	What is periodic location updating and what is the need of periodic location updating? Explain how periodic updating is done in GSM. ➢ Need for Location updating: • It should be possible for the MS to receive a call from the network at any time at any location. • While the MS moves freely within a network, the network should	L3

know about its whereabouts, in terms of its location and the cell with which it is attached.

- The MS should update the network whenever it changes the location and is called Location Updating.
- Three types of location updating:

1. Location updating normal.
2. IMSI attach.
3. Periodic Registration.

Location updating Normal



- A location area is the area handled by one or more BTSs where the MS can move around without updating the network.
- A location area is controlled by one or more BSCs but strictly by one MSC.
- MS gets the location area identity of the serving cell, through listening the BCCH.
- MS compares the Location Area Identity (LAI) to the one stored in the MS through the SIM card & if LAI differs from the one stored in the SIM card, the MS decides to do a location update, type normal.

1. The MS listens to the system information on BCCH Channel, compares the LAI with the one stored in SIM card. When it finds the difference, it decides to do an location update.

2 a. The MS sends a channel request message through RACH channel.

2 b. The message received by the BTS is forwarded to the BSC. The BSC allocates a SDCCH, if there is one idle, and tells the BTS to activate it.

2 c. BTS give acknowledgement on AGCH channel.

3 . The MS sends a location updating request message which contains the identity of the MS, the identity of the old location area and the type of

updating.

4a. The authentication parameter is sent to the MS. If the MS is not already registered in this MSC/VLR the appropriate HLR or the previously used MSC/VLR must be contacted to retrieve MS subscriber data and authentication parameters.

4b. MS sends an answer calculated using the received authentication parameter.

If authentication is successful, the VLR is updated.

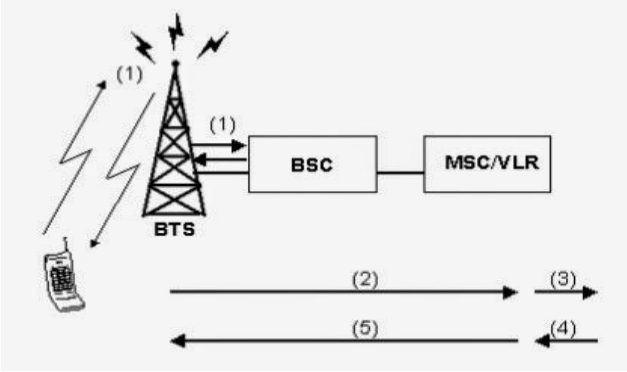
6. The MS receives an acceptance of the location updating.

7a. The BTS is told to release the SDCCH.

7b. The MS is told to release the SDCCH and switches to idle mode.

During the location change, if the MS is busy in call, it receives the information about the new LAI on the SDCCH. The location updating (above said procedure) takes place after the call is released

Location Updating IMSI attach



- MSI attach is used by the MS to notify the system that it was powered on, provided it is still
- in the same location area as it was when it entered the detached state.
- This procedure is to be used only when the IMSI detach flag is set in the VLR.
- If the flag is set in the HLR, switching to active mode
- requires a normal location updating of the MS.

1. The MS requests a SDCCH (The point number 1 , 2a, 2b , 2c all are same as in Normal Updating).

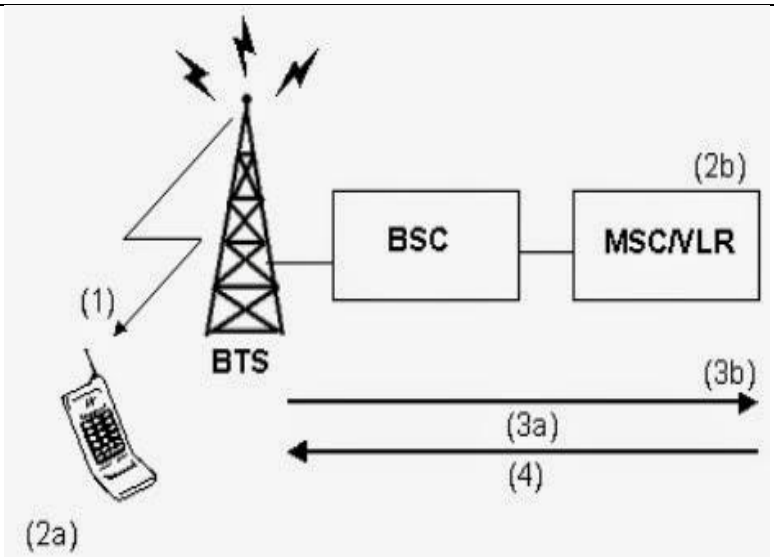
2. The system receives the IMSI attach message from the MS.

3. The MSC sends the IMSI attach message to the VLR. The VLR removes the IMSI detached flag and resumes normal call handling for the MS.

4. The VLR returns the IMSI attach acknowledge message to the MSC.

5. The MS also receives an acknowledge message.

Location Updating Periodic Registration

	 • Periodic registration is a type of location updating procedure that is used to avoid unnecessary paging of the mobile in cases where the MSC never receives the IMSI detach message and also to prevent damage in case of database failure. 1. The MS is informed via the system information if periodic registration is used in the cell. If periodic registration is used, the MS is told how often it must register. The time is set by a counter where the values are 0 to 255 deci-hours (a unit of six minutes). If the parameter is set to zero means periodic registration is not used, if the parameter is set to twenty for example, then MS must register every two hours. 2. The procedure is controlled by a timer both in the MS and in MS. 3. When the timer in the MS expires, the MS performs a location updating, type periodic registration and the timers in MS and MSC restart. 4. In the MSC there is a time scanning function for the MS, if the MS does not register within the determined interval plus a guard time, then the scanning function in MSC detects this and the MS is flagged as detached.	
7.	Bring out the difference between intra-BSC handover and inter-BSC handover using appropriate figures. Check solution in Q13	L3
8.	Bring out the difference between inter-BSC handover and inter-MSC handover using appropriate figures. Check solution in Q13	L3
9.	What are the basic functions of connection management sub layer? Check solution in Q13	L1
10.	What are the basic functions of mobility management sub layer?	L2

	Check solution in Q15	
11.	What are the basic functions of radio resource sub layer? Check solution in Q15	L3
12.	What is LAPD and why is a modified version of LAPD necessary for Um interface. Check solution in Q15	L2
13.	Categorize the various handovers in GSM. One of the key elements of a mobile phone or cellular telecommunications system, is that the system is split into many small cells to provide good frequency re-use and coverage. However as the mobile moves out of one cell to another it must be possible to retain the connection. The process by which this occurs is known as handover or handoff . The term handover is more widely used within Europe, whereas handoff tends to be use more in North America. Either way, handover and handoff are the same process. Requirements for GSM handover The process of handover or handoff within any cellular system is of great importance. It is a critical process and if performed incorrectly handover can result in the loss of the call. Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network. Accordingly GSM handover was an area to which particular attention was paid when developing the standard. ➢ **Types of Handover:** 1. *Intra-BSC handover:* 2. *Inter-BSC handover:* *3. Inter-MSC handover:* *Intra-BSC handover:*	L3

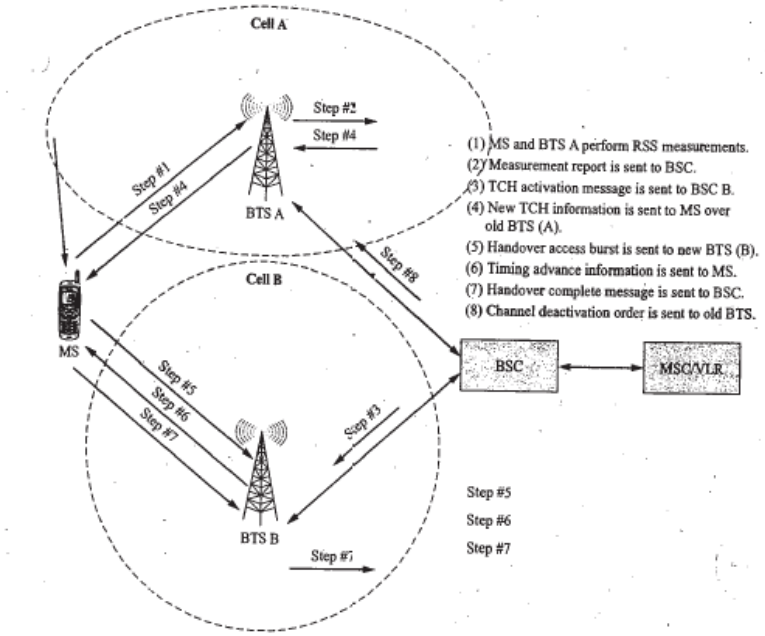
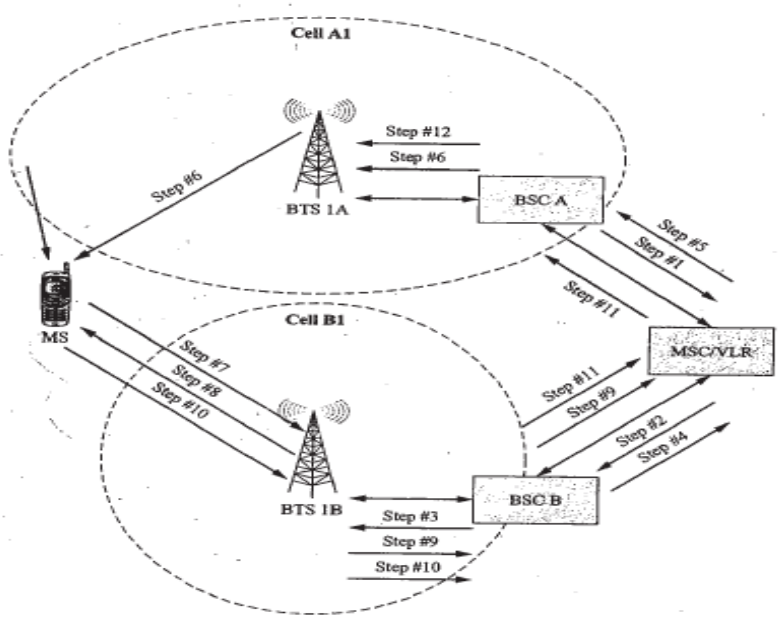


Figure 5–42 GSM Intra-BSC handover (Courtesy of Ericsson).

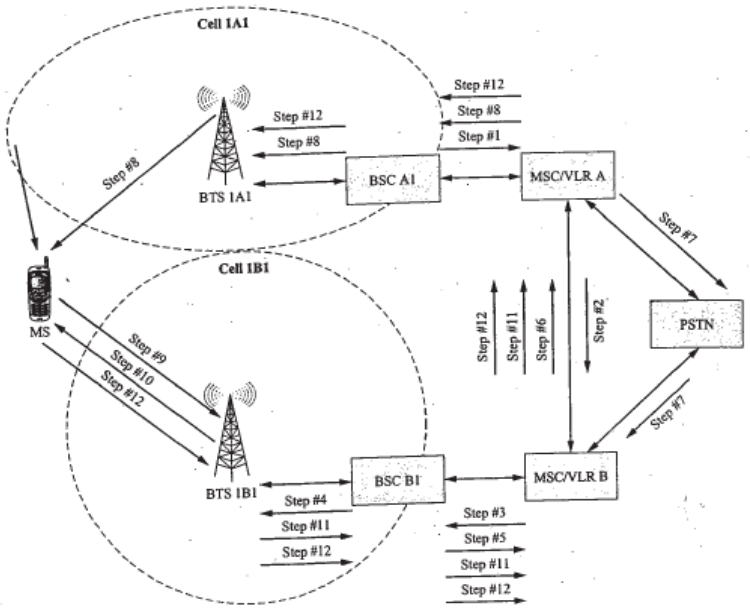
Inter-BSC handover:



(1) Handover request is sent by serving BSC to MSC.

(1) Handover request is sent by serving BSC to MSC.
(2) Handover request is sent by MSC to new BSC (B).
(3) BSC B sends activation order to BTS 1B.
(4) BSC B sends handover information to MSC.
(5) MSC sends handover information to BSC A.
(6) BSC A sends MS new TCH information.
(7) MS sends handover access burst to new BTS (1B).
(8) Timing advance information is sent to the MS.
(9) BTS 1B sends handover detection message to BSC B.
(10) MS sends handover complete message to BSC B.
(11) BSC B sends handover complete message to the old BSC (A).
(12) Old BSC (A) sends channel deactivation message to old BTS (1A).

Inter-MSC handover:



	(1) Handover request is sent by serving BSC (A1) to MSC A. (2) MSC A requests assistance from MSC B. (3) MSC B provides MSC A with handover number and sends new BSC (B1) a handover request. (4) New BSC (B1) sends handover activation order to new BTS (1B1). (5) BSC sends handover information to new MSC. (6) Handover information is send to old MSC. (7) A signaling/traffic link is set up between the two MSCs. (8) Handover message is sent to MS. (9) MS sends handover access burst to new BTS. (10) New BTS sends timing advance information to MS. (11) Old MSC is sent handover detected message. (12) MS sends handover complete message to new BSC. BSC sends handover complete message to the old BSC. Old BSC sends channel deactivation message to old BTS (1A1).	
14.	Discuss the various security algorithms GSM provides. A consequence of international roaming is the exchange of information between providers in different countries. All countries have strict regulations against the export of encryption algorithms and thus GSM works around it. When a user tries to use his phone in say another country, the local networks request the HLR of the subscriber's home network for the RAND, SRES and KC which is sufficient for authentication and encrypting data. Thus the local network does not need to know anything about the A3 or A8 algorithms stored in the SIM. ***Authentication Algorithm A3*** – It is operator dependent and is an operator option. The A3 algorithm is a oneway function. That means it is easy to compute the output parameter SRES by using the A3 algorithm but very complex to retrieve the input parameters (RAND and KI) from the output parameter. Remember the key to GSM's security is keeping KIunknown. While it maysound odd that each operator may choose touse A3 independently, it was necessary tocover the case of international roaming. ***Ciphering Algorithm A5*** - Currently, there exists several implementations of this algorithm though the most commonly used ones are A5/0, A5/1 and A5/2. The reason for the different implementations is due to export restrictions of encryption technologies. A5/1 is the strongest version and is used widely in Western Europeand America, while the A5/2 is commonlyused in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption. ***Ciphering Key Generating Algorithm A8 –*** It is operator dependent. In most providers the A3 and A8 algorithms are combined intoa single hashfunction known as COMP128. The COMP128 creates KCand SRES, in a single instance. **OR (Decide based on Marks)**	L1

	In GSM, security is implemented in three entities: SIM card, GSM handset and Network. Subscriber identity module (SIM) contains: -IMSI - TMSI -PIN, -MSISDN -Authentication key Ki (64-bit) -Ciphering key (Kc) generating algorithm A8, and -Authentication algorithm A3. SIM is a single chip computer containing the operating system (OS), the file system, and applications. SIM is protected by a PIN and owned by an operator. SIM applications can be written with a SIM tool kit. **GSM handset** contains ciphering algorithm A5. **Network** uses algorithms • A3 for Authentication, • A5 for encryption: A5 is a stream cipher. It can be implemented very efficiently on hardware. Its design was never made public. A5 has several versions: A5/1 (most widely used today), A5/2 (weaker than A5/1; used in some countries), and A5/3 (newest version based on the Kasumi block cipher). • A8 for ciphering the data; Ki and IMEI and IMSI of each subcriber are stored in the authentication center. Both A3 and A8 algorithms are implemented on the SIM. The operator can decide which algorithm is to be used. Implementation of an algorithm is independent of hardware manufacturers and network operators. **1. Authentication of GSM mobiles:** Authentication in the GSM system is achieved by the Base Station sending out a challenge to the mobile station. The MS uses a key stored on its SIM to send back a response that is then verified. This only authenticates the MS, not the user.	

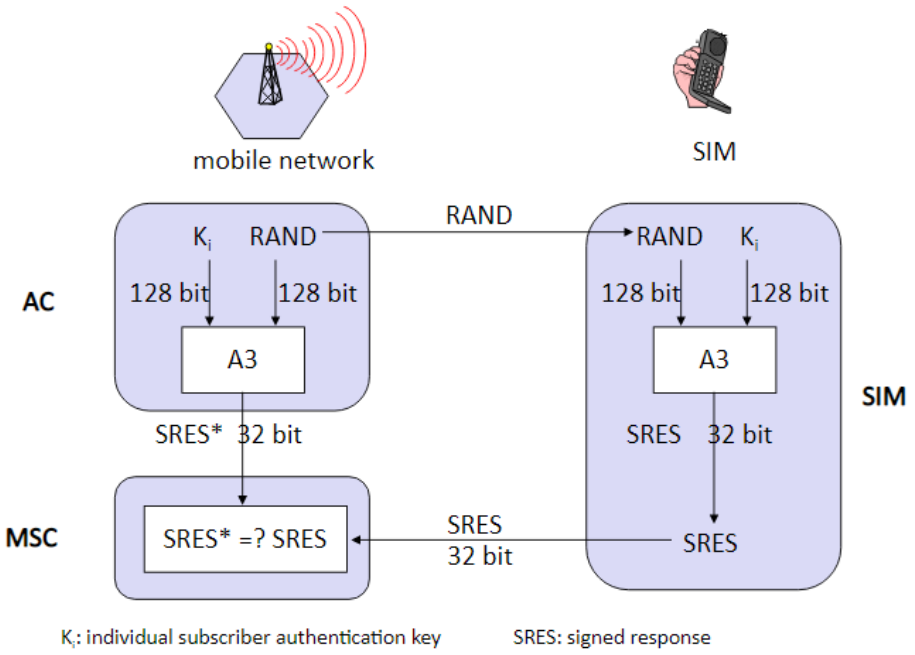


Figure 15: process of authentication in GSM

To request for a call or to receive a call, the MS has to get authenticated. The process is as follows:

- A unique subscriber authentication key is programmed on every SIM card. The authentication center (AuC) has a list which maps Ki number with the SIM card.It is a secure database.
- When a SIM card requests for a call, a 128 bit random number is instantaneously generated by the AuC and transmitted to the SIM card.
- The A3 algorithm which is programmed inside the SIM card processes the RAND number and Ki number and generates a 32 bit output called the Signed RESponse number (SRES).
- The same process is done on the AuC side.
- The SIM card transmits this SRES number to the AuC.
- The AuC compares the received SRES with the SRES that's generated on the network side.
- The SIM is authenticated if and only if the two SRES are same.

The authentication centre contains a database of identification and authentication information for subscribers including IMSI, TMSI, location area identity (LAI), and authentication key (Ki). It is responsible for generating (RAND),response (RES), and ciphering key (Kc) which are stored in HLR / VLR for authentication and encryption processes. The distribution of security credentials and encryption algorithms provides additional security.

2. Encryption in GSM:

GSM uses information stored on the SIM card within the phone to provide encrypted communications and authentication. GSM encryption is only applied to communications between a mobile phone and the BS. The rest of the transmission over the normal fixed network or radio relay is unprotected, where it could easily be eavesdropped or modified. In some countries, the base station encryption facility is not activated at all, leaving the user completely unaware of the fact that the transmission is not secure. GSM encryption is achieved by the use of a shared secret key. If this key is compromised it will be possible for the transmission to be eavesdropped and for the phone to be cloned (i.e., the identity of the phone can be copied). A 64-bit key is divided to provide data confidentiality. It is not possible to encrypt all the data; for example, some of the routing information has to be sent in clear text. The detailed process of Encrypting the data is as shown in Figure 16.

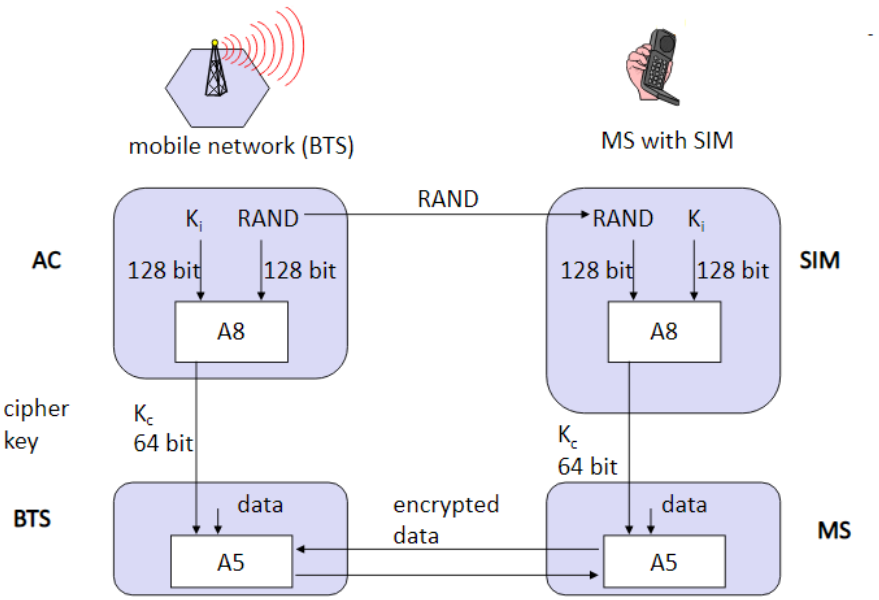


Figure 16: process of authentication in GSM

- The AuC generates a random number (RAND) of 128 bits and sends it to the MS.
- The RAND and the Ki number is processed by the A8 algorithm on both the sides.
- The A8 algorithm produces a 64 bit ciphering key (Kc). Ciphering means scrambling or randomizing the data.
- The A5 algorithm takes Kc key and data to be transmitted as input and and accordingly encrypts the data.
- A5 algorithm is different for each service provider and is highly secretive.

3. GSM Token-based challenge

The security-related information consisting of triplets of RAND, signature response (SRES), and Kc are stored in the VLR. When a VLR has used a token to authenticate an MS, it either discards the token or marks it used. When a VLR needs to use a token, it uses a set of tokens that is not marked as used in preference to a set that is marked used. When a VLR successfully requests a token from the HLR or an old VLR, it discards any tokens that are marked as used. When an HLR receives a request for tokens, it sends any sets that are not marked as used. Those sets shall then be deleted or marked as used. The system operator defines how many times a set may be reused before being discarded. When HLR has no tokens, it will query the authentication centre for additional tokens. The token-based challenge can be integrated into various call flows (e.g., registration, handoff). It is described separately here for clarity. Figure 17 shows the call flows of token-based challenges.

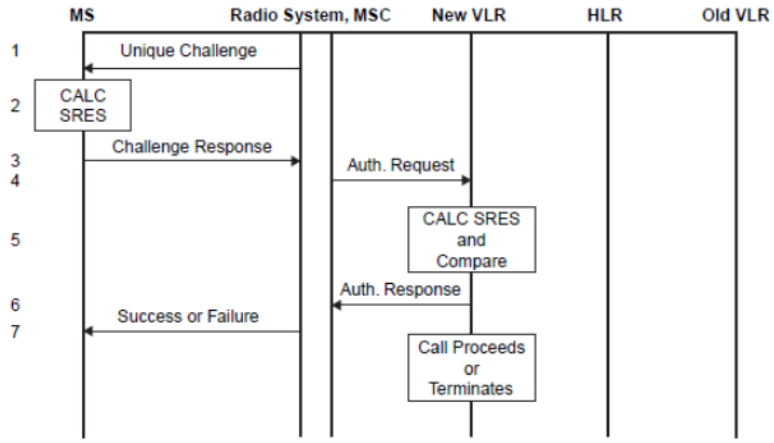
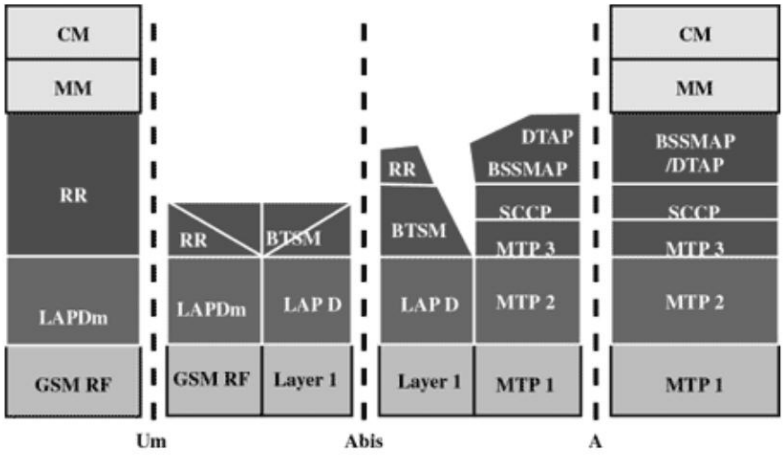


Figure 17: GSM token-based challenge

- The serving system sends a RAND to the MS.
- The MS computes the SRES using RAND and the authentication key (Ki) in the encryption algorithm.
- The MS transmits the SRES to the serving system.
- The MSC sends a message to the VLR requesting authentication.
- The VLR checks the SRES for validity.
- The VLR returns the status to the MSC.
- The MSC sends a message to the MS with a success or failure indication.

Both GSM and North American systems use the international mobile equipment identity (IMEI) stored in the equipment identity register (EIR) to check malfunctions and fraudulent equipment. The EIR contains a valid list (list of valid mobiles), a suspect list (list of mobiles

	under observation), and a fraudulent list (list of mobiles for which service is barred).	
15.	**Explain the GSM protocol Stack and function of each layer.** **GMS protocol stacks diagram is shown below:**  **MS Protocols:** Based on the interface, the GSM signaling protocol is assembled into three general layers: • **Layer 1:** The physical layer. It uses the channel structures over the air interface. • **Layer 2:** − The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used. • **Layer 3:** GSM signalling protocol's third layer is divided into three sublayers: Radio Resource Management (RR), Mobility Management (MM), and Connection Management (CM). **MS to BTS Protocols:** The RR layer oversees the establishment of a link, both radio and fixed, between the MS and the MSC. The main functional components involved are the MS, the BSS, and the MSC. The RR layer is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels, including the allocation of dedicated channels. The MM layer is built on top of the RR layer and handles the functions that arise from the mobility of the subscriber, as well as the	L2

authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

The CM layer is responsible for CC, supplementary service management, and Short Message Service (SMS) management. Each of these may be considered as a separate sublayer within the CM layer. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC Protocols:

After the information is passed from the BTS to the BSC, a different set of interfaces is used. The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM). The BTS management layer is a relay function at the BTS to the BSC.

The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination. The RR protocols provide the procedures for the use, allocation, reallocation, and release of the GSM channels. The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.

From the BSC, the relay is using SS7 protocols so the MTP 1-3 is used as the underlying architecture, and the BSS mobile application part or the direct application part is used to communicate from the BSC to the MSC.

MSC Protocols:

At the MSC, the information is mapped across the A interface to the MTP Layers 1 through 3 from the BSC. Here, the equivalent set of radio resources is called the BSS MAP. The BSS MAP/DTAP and the MM and CM are at the upper layers of Layer 3 protocols. This completes the relay process. Through the control-signaling network, the MSCs interact to locate and connect to users throughout the network. Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Each user of a GSM MS is assigned a HLR that is used to contain the user's location and subscribed services. A separate register, the VLR,

	is used to track the location of a user. As the users roam out of the area covered by the HLR, the MS notifies a new VLR of its whereabouts. The VLR in turn uses the control network (which happens to be based on SS7) to signal the HLR of the MS's new location. Through this information, MT calls can be routed to the user by the location information contained in the user's HLR.	