GSM

Syllabus

2.1 GSM Mobile services, System Architecture, Radio interface, Protocols , Localization and Calling, Handover, security (A3, A5 & A8)

2.2 GPRS system and protocol architecture

2.2 UTRAN, UMTS core network; Improvements on Core Network

2.1 GSM

Global System for Mobile communication (GSM) is the most successful digital mobile telecommunication system in the world today. It is used by over 1000 million people in more than 190 countries. The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice service that is compatible to ISDN and PSTN. This chapter gives an insight of GSM system including its services, architecture, call set up procedure, handover and other important aspects such as security and authentication.

2.1.1 GSM Overview

MU - Dec. 12

Q. List and explain GSM services. **(Dec. 12, 5 Marks)**

- Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. It is an ETSI standard for 2G pan-European digital cellular system with international roaming.
- The basic version of GSM (i.e. GSM 900) was founded in 1982.
- Now it is the most successful mobile communication system in the world and over 1.2 billion users use the system.
- The main goal of GSM was to provide voice services that are compatible to ISDN and other PSTN systems at the same time allowing users of the system to roam throughout Europe.
- GSM is a second generation 2G system, replacing the first generation analog systems.
- The initial version of GSM was designed in Europe using **890-915MHZ** for **uplink** and **935-960 MHz** for **downlink.** This system is called **GSM 900.**
- Another version of GSM called Digital Cellular System 1800 (DCS 1800) uses 1710-1785 MHz for uplink and
- 1805-1880 MHz for downlink.
- GSM at 1900 MHz (1850-1910 MHz uplink and 1930-1990 MHz downlink) used in US is called PCS (Personal Communication Services) 1900.

Modifications and Derivatives of GSM

- The system evolution of GSM can be divided into three phases.
  - **Phase 1 (1991-1994) :** The basic version of the GSM system was in operation.

- **Phase 2 (1994-1995) :** The system specification was verified in order to allow future gradual modifications and new improvements.
- **Phase 3 (from 1995) :** The modifications to the original GSM900 are being introduced.

– Following are the derivatives of the original GSM 900.

DCS 1800

– One important modification to the original GSM900 was the development of **Digital Cellular System** (DCS 1800).

– DCS 1800 is primarily devoted to the operation in areas with high traffic such as urban and suburban areas.

– It is called as DCS in United Kingdom and PCS in Hong Kong.

– The main difference between GSM900 and DCS1800 was in the lower power of the base station and mobile station. As a result the cell size becomes smaller.

– The bandwidth assigned to the DCS1800 was much higher than the GSM900. This implies that up to 374 carrier frequency channels can be assigned to the DCS1800. Thus the capacity of DCS1800 is much higher than the GSM900. But this also implies twice as high sensitivity to Doppler effects. This limits the maximum vehicle speed in DCS1800 up to 130km/hr.

– Another essential enhancement of the DCS1800 is the possibility of roaming inside the country. This was not possible with initial GSM900 due to organization reason.

– Table 2.1.1 summarizes the basic difference between GSM900 and DCS1800.

Table 2.1.1 : Difference between GSM 900 and DCS 1800

Feature	GSM 900	DCS 1800
Frequency range	Uplink 890-915 MHz Downlink 935-960 MHz	Uplink 1710-1785 MHz Downlink 1805-1880 MHz
Number of duplex channels	124	374
Maximum Base station power	320W	20W
Maximum Mobile station power	8W	1W
Spacing between uplink and downlink frequencies	45MHz	95MHz
Maximum vehicle speed	250km/hr	130km/hr
MS classes	20W (not implemented) 8W (car/ transportable phone) 5W (car/ transportable phone) 2W (handheld) 0.8 W (handheld	1W (handheld) 0.25 W (handheld)

– Table 2.1.2 lists the key milestones of the GSM system and its derivatives.

GSM 400

– Another promising modification and enhancement of the original GSM 900 system was GSM 400. It has been observed that the analog systems operating in the 400 MHz bands are now becoming absolute. They are losing their customers as most of them moved to the 2G systems.

- After shutting these analog systems completely, this frequency range can be used for another GSM version.
- ETSI standardized the GSM system operating in the band around 450 and 480 MHz called GSM 400.
- The whole infrastructure will remain same however software needs to be changed.
- The basic feature of GSM 400 are listed below:
  - Frequency allocation : Uplink : 450.4-457.6 MHz
    Downlink : 460.4-496.0 MHz
  - Duplex separation : 10 MHz
  - Carrier spacing : 200KHz

Table 2.1.2 : Key milestones of the GSM system and its derivatives

Year	Milestone
1982	Groupe Special Mobile established by CERT to develop the pan-European cellular mobile system standards.
1985	Basic list of recommendations to be generated by the group was adopted.
1986	Field tests undertaken to prove which techniques should be adopted for the new system.
1987	TDMA approach adopted as the main access method for GSM. Frequency division is also used between channels, but time division is used in each individual frequency channel.
1988	GSM system validation undertaken.
1989	ETSI, European telecommunications Standards Institute takes on responsibility for managing the GSM standards.
1990	Phase 1 of the GSM specifications released.
1991	Commercial launch of the GSM service.
1993	Coverage of main roads GSM services start outside Europe.
1995	Phase 2 of the GSM specifications released.
2004	GSM subscriptions reach 1 billion.

2.1.2 Mobile Services

- GSM is an integrated voice-data service that provides various services beyond cellular telephone.
- GSM Mobile services are divided into categories.
  1. Bearer services
  2. Tele services
  3. Data services
  4. Supplementary services
- Fig. 2.1.1 shows the reference model of GSM Mobile teleservices and bearer services.

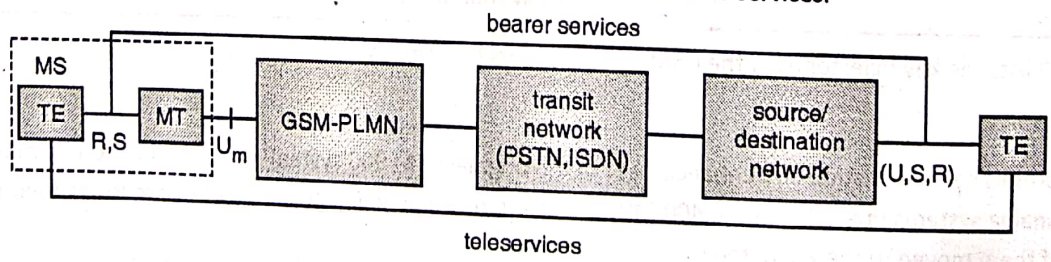

Fig. 2.1.1 : GSM Mobile services

1. Bearer services

- Bearer services are telecommunication services that provide capabilities to transfer user data and control signals between two pieces of equipment in a network.
- GSM provides basically four types of bearer services :
  - Transparent
  - Non-transparent
  - Synchronous data transmission
  - Asynchronous data transmission

(i) Transparent bearer services

- These types of bearer services use the functions of physical layer to transmit data.
- To improve the transmission quality, it uses forward error correction (FEC) at physical layer.

(ii) Non-transparent bearer services

- Non transparent bearer services use functions of both layer 2 and layer 3 to improve transmission quality.
- It implements layer 2 and layer 3 protocols for error correction and flow control.
- It also uses radio-link protocol (RLP) that comprises mechanism of **High Speed Data Link Control (HDLC)** and special **selective-reject** mechanism to trigger retransmission of data.
- The bit-error rate is less than 10^{-7}, and throughput and delay may vary depending upon transmission quality.
- Different data rates for voice and data that can be achieved are listed below.

2. Data Services

(i) Data service (circuit switched)

- Synchronous : 2.4, 4.8 or 9.6 kbit/s
- Asynchronous: 300 - 1200 bit/s

(ii) Data service (packet switched)

- Synchronous : 1.2, 2.4, 4.8 or 9.6 kbit/s
- Asynchronous : 300 - 9600 bit/s

3. Tele services

- Tele services include encrypted voice transmission, message services, and basic data communication with terminals.
- The GSM was basically designed to provide high quality digital voice transmission, offering at least the bandwidth
- 3.1 kHz of analog phone systems.

The various teleservices are :

(i) Emergency number

- It is mandatory for all service providers to implement Emergency number service.
- This number is the common number that can be used throughout country.
- Like police (100) or ambulance number and this number is free of charge.
- This connection has the highest priority and will automatically be set up with closest emergency center.

(ii) Short message services (SMS)

- SMS allows transmission of text messages up to 160 characters.

- SMS uses unused capacity in the signaling channels instead of standard data channels.
- It is possible to send or receive SMS during voice or data transmission.
- SMS can be used for displaying road conditions, e-mail headers or stock quotes etc.
- SMS are also used for updating mobile phone software or for implementation of push services.

(iii) Enhanced Message Service (EMS)

Enhanced message service (EMS) allows transmission of larger messages, formatted text, animated pictures, small images, and ringtones in a standardized way.

(iv) Multimedia Message service (MMS)

MMS allows transmission of larger pictures such as JPEG, GIF, WBMP files and also short video clips.

(v) Group 3 Fax

- In this service, fax data is transmitted as digital data over the analog telephone network using modems.
- It uses ITU-T standards T.4 and T.30 for transmission.
- Fax data and fax signaling is transmitted via transparent bearer service.

4. Supplementary services

- Supplementary services offer various enhancements of the standard telephony services and may vary from provider to provider.
- Supplementary services are additional services that are provided by the GSM system other than teleservices or bearer services.
- These services include facilities such as call forwarding, caller identification, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. Some supplementary services are :
  - Multiparty Service or conferencing
  - Call Waiting
  - Call Hold
  - Call Forwarding
  - Call Barring
  - Number Identification
  - Advice of Charge (AoC)
  - Closed User Groups (CUGs)
  - Unstructured supplementary services data (USSD) : This allows operator-defined individual services.

Table 2.1.3 : GSM services

Service Category	Service
Tele services	Telephony
	Emergency call
	Short message services
	Videotext access
	Teletex, Fax
	Half rate speech coder
	Enhanced full rate

Service Category	Service
Bearer services	Synchronous data Asynchronous data Synchronous packet data
Supplementary services	Call forwarding Call barring Calling line identification Connected line identification Call waiting Call hold Multiparty communication Closed user group Advice of charge Operator determined call barring

2.1.3 GSM System Architecture

MU - Dec. 12, May 13

Q. Draw a neat diagram of GSM system architecture and explain with different types of interfaces. **(Dec. 12, 10 Marks)**

Q. What is the use of HLR and VLR registers in Mobile computing? **(May 13, 5 Marks)**

- Fig. 2.1.2 shows the simplified view of the GSM system architecture.
- The GSM network architecture can be grouped into three main sub systems :

1. Radio subsystem (RSS)
2. Network and switching subsystem (NSS)
3. Operation subsystem (OSS)

1. Radio subsystem

Radio subsystem comprises all radio entities. Entities of RSS are explained below.

(i) Base station subsystem (BSS)

- A GSM network comprises many BSSs.
- BSS contains one or more radio cells, each one is controlled by a base transceiver station (BTS).
- One or more BTSs in turn are controlled by an element called Base station controller (BSC). Thus there are two main architectural elements in each BSS **BTS** and **BSC.**
- **BSS functions** are to :
  - Maintain radio connection to MS
  - Coding/decoding of voice
  - Rate adaptation to/from the wireless network part

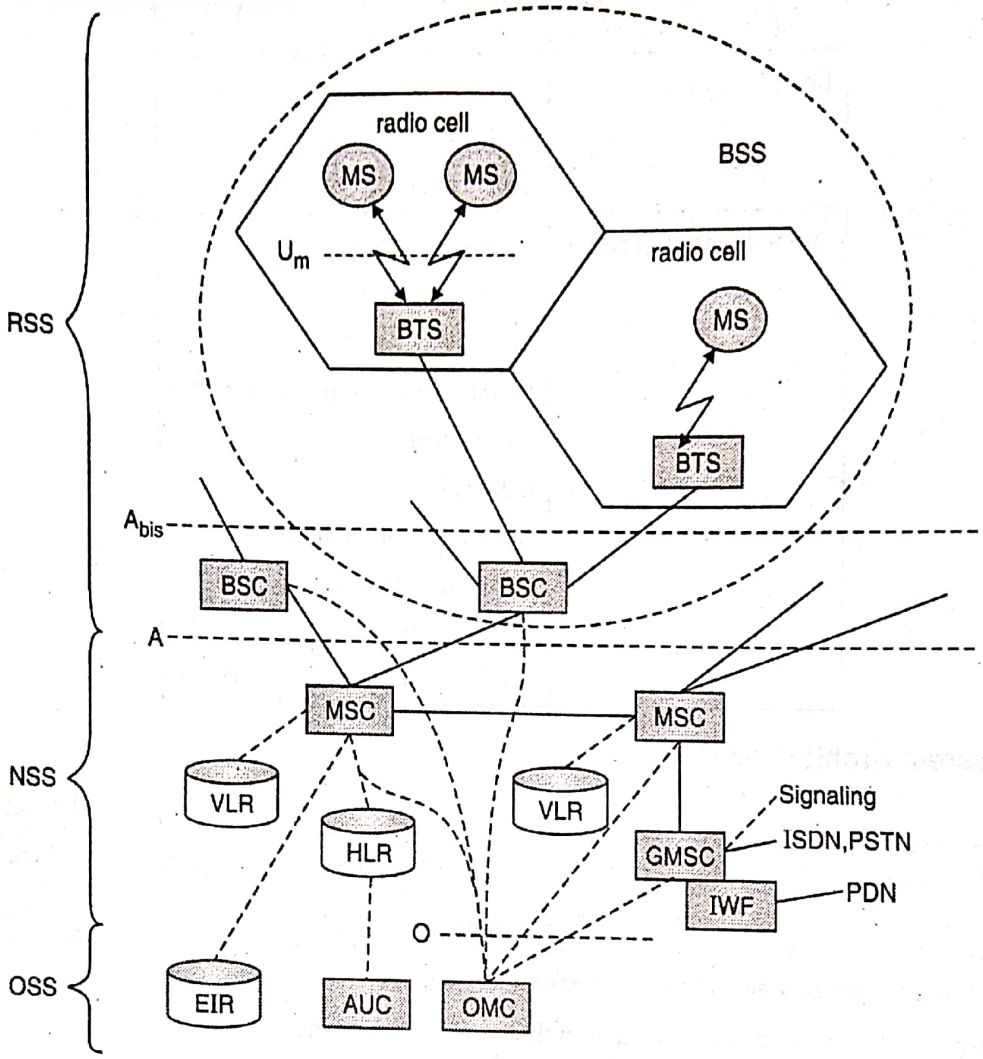

Fig. 2.1.2 : GSM system architecture

(ii) Base transceiver station (BTS)

- A BTS (also called base station) comprises all radio equipments, i.e. antennas, signal processing, amplifiers etc.
- BTS can form a single radio cell or several cells by using sectorized antennas.
- BTS is connected to MS via the **U_m interface** and to the BSC via the **A_{bis} interface**.
- **Functions of BTS** are :
  - Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
  - Transcoding and rate adaptation
  - Time and frequency synchronization
  - Voice through full- or half-rate services
  - Decoding, decrypting, and equalizing received signals
  - Random access detection
  - Uplink channel measurements

(iii) Base station controller (BSC)

- The BSC manages the radio resources for one or more BTSs.
- **Functions of BSC** are :
  - Handles radio channel setup, frequency hopping, and handovers.

- Assigns and releases frequencies and time slots for the MS.
- Handles inter cell handover.
- Controls the power transmission of the BSS and MS in its area.

– **Additional functions** include :
- Performing traffic concentration to reduce the number of lines from the MSC
- Reallocation of frequencies among BTSs
- Time and frequency synchronization
- Power management
- Time-delay measurements of received signals from the MS

(iv) Mobile station (MS)

– The MS comprises all user hardware and software needed for communication with a GSM network.

– International mobile equipment identity (IMEI) is used to identify an MS. Device specific mechanism like theft protection uses the IMEI number.

– MS consists of two elements mobile equipment (ME) and SIM.

– Mobile equipment (ME) is the hardware that is the mobile handset.

– The second component of MS is **subscriber identity module (SIM).**

– SIM stores all user specific data relevant to GSM.

– All the calls in GSM are SIM based and they are directed to the SIM rather than terminal.

– All the data like SMS, contact numbers are also stored in SIM card.

– User specific functions like charging, authentication are also based on the SIM.

– Without SIM only emergency calls are possible.

– The SIM card contains many identifiers, and tables such as card type, serial number, a list of subscribed services,

– **A Personal Identification Number (PIN), PIN Unblocking Keying (PUK),** an **authentication key K_i** and the **International Mobile Subscriber Identity (IMSI).**

– The mobile station also stores the dynamic information while logged onto the GSM system such as **cipher key K_c** and a **Temporary Mobile Subscriber Identity (TMSI),** and the **Location Area Identification (LAI).**

2. Network and Switching Subsystem (NSS)

– The NSS connects the radio network with the standard public mobile networks.

– The NSS includes the main switching functions of GSM, important databases (such as HLR, VLR) required to manage user profile and user mobility.

– The NSS contains the following functional elements.

(i) Mobile service switching center (MSC)

– MSC is the heart of the GSM architecture.

– They are high-performance digital ISDN switches.

– Each MSC controls one or more BSSs.

– MSC sets up the connections to other MSCs and to the BSCs via the **A interface.**

The MSC performs following functions

- Switching of calls between the mobile and other fixed or mobile network users
- Management of mobile services
- Registration
- Authentication
- Location updating
- Handovers
- Call routing to a roaming subscriber
- Toll ticketing
- Network interfacing
- Common channel signaling

– MSCs are connected with each other and also to the Gateway MSCs (GMSC).

– **Gateway MSC** is responsible for communication with the external fixed networks such as PSTN and ISDN.

– MSC can also connect to public data networks (PDN) such as x.25 by using additional interworking functions (IWF).

(ii) Home Location Register (HLR)

– The HLR register is the central database that stores and manages the permanent information of the subscriber.

– When an individual buys a subscription in the form of SIM, all the information about this subscription is registered in the HLR of that operator.

– HLR contains the following static and dynamic information.

(a) Static information

- Mobile subscriber ISDN number (MSISDN)
- International mobile subscriber identity (IMSI)
- List of services to which user has subscribed such as call forwarding, roaming restriction, GPRS etc.

– All these user-specific information is entered once for each user in a single HLR at the time of subscription.

– HLR also maintains some dynamic information that is used for locating the user.

(b) Dynamic information

- The current location area (LA) of MS
- The mobile subscriber roaming number (MSRN)
- Current VLR and MSC

– As soon as MS leaves its current LA, the VLR that is currently responsible for the MS informs HLR about its new location.

(iii) Visitor Location Register (VLR)

– The VLR is associated to each MSC.

– It is a database containing records of all mobile stations currently registered with the attached MSC.

– When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR.

– Later if the mobile station makes a call, the VLR need not contact HLR each time since the VLR has all the information needed to set up the call.

– The VLR avoids the frequent HLR access/updates, as all the user information required is available in VLR.

3. Operation Sub System (OSS)

- The OSS is the functional entity which is used to monitor and control the overall GSM network.
- It is also used to control the traffic load of the BSS.
- OSS contains the following entities.

(i) Operation and Maintenance Center (OMC)

- The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC.
- The OMC monitors and controls all other network entities via the ***O interface***.
- Here are some of the OMC functions :
  - Administration and commercial operation (subscription, end terminals, charging and statistics).
  - Security Management.
  - Network configuration, Operation and Performance Management.
  - Maintenance Tasks.
  - Traffic monitoring
  - Status reports of network entities

(ii) Authentication Center (AUC)

- The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.
- The AUC protects network operators from different types of fraud.
- AUC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.

(iii) Equipment Identity Register (EIR)

- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipments on the network. It stores International Mobile Equipment Identity (IMEI) number for each valid mobile equipment.
- The EIR has a black list of stolen mobile devices.
- If a particular mobile is stolen or is not type approved then corresponding IMEI is marked as invalid in the EIR.

MU - Dec. 15

2.1.4 GSM Radio Interfaces

Q. Explain the U_m interface of GSM. **(Dec. 15, 5 Marks)**

Different elements of GSM network communicate to each other using well defined interface between them.

Um Interface :

- The **U_m interface** is the **air interface** for the **GSM** mobile telephone standard.
- It is the **interface** between the mobile station (MS) and the Base transceiver station (BTS).
- It is called **Um** because it is the mobile analog to the U **interface** of ISDN.
- **Um** is **defined** in the **GSM** 04.xx and 05.xx series of specifications.
- The GSM air interface is based on Time Division Multiple Access (TDMA) with Frequency Division Duplex (FDD).
- TDMA allows multiple users to share a common RF channel on a time-sharing basis, while FDD enables different frequencies to be used in uplink (MS to BTS) and downlink (BTS to MS) directions.

- Most of the implementations use a frequency band of 900 MHz. The other derivative of GSM is called Digital cellular system uses 1800 MHz (DCM1800).
- The used frequency band is divided into 200KHz carriers or RF channels in both the uplink and downlink direction.
- Each RF channel is then further subdivided into eight different timeslots, i.e., 0 to 7, by TDMA techniques.
- A set of these eight timeslots is referred to as a TDMA frame.
- Each frame lasts 4.615 msec.
- The physical channels are further mapped to various logical channels carrying user traffic and control information between the MS and the BTS.
- The following section describes the Um interface protocols used at the MS and the BTS side.

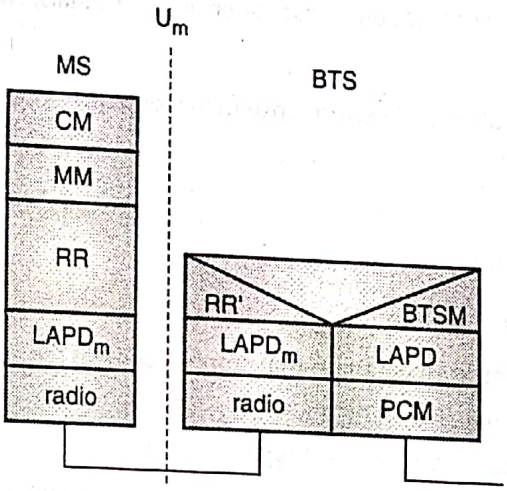

Fig. 2.1.3 : The Um interface between MS and BTS

Physical layer

Layer 1, which is a radio interface, provides the functionality required to transfer the bit streams over the physical channels on the radio medium. The services provided by this layer to the above layers include :

- Channel mapping (logical to physical)
- Channel coding and ciphering
- Digital modulation
- Frequency hopping
- Timing advance and power control

Data link layer

- Signaling Layer 2 is based on the LAPDm protocol, which is a variation of the ISDN LAP-D protocol.
- The main task of LAPDm is to provide a reliable signaling link between the network and the mobile station.
- The LAP-D protocol has been modified to adapt in the mobile environment.

Network layer

- Signaling Layer 3 takes care of signaling procedures between an MS and the network. It consists of three sublayers with distinct signaling procedures.
  - Radio resource management (RR)
  - Mobility management (MM)
  - Connection management (CM)

- Radio resource management (RR) comprises procedures required to establish, maintain, and release the dedicated radio connections. The RR sub layer functions include :
  - Channel assignment and release
  - Ciphering
  - Modification of channel modes, e.g., voice and data
  - Handover between cells
  - Frequency redefinition to enable frequency hopping
  - MS measurement reports
  - Power control and timing advance
  - Paging
  - Radio channel access
- The mobility management (MM) sublayer handles functions and procedures related to mobility of the mobile user. This includes procedures for Authentication and Location registration and periodic updating.
- The connection management (CM) sublayer contains the functions and procedures for call control. This includes procedures to establish, release, and access services and facilities.

(i) **A_{bis} Interface :** BSC and BTS communicate via A_{bis} interface. The A_{bis} interface is associated with the information exchange related to the radio transmission such as distribution of radio channels, connection supervising, the queuing of messages before transmission, frequency hopping control, channel coding, decoding etc.

(ii) **A interface :** The A interface is used to provide communication between the BSS and the MSC. It is based on **circuit switched PCM-30** systems. It carries up to 3064 kbits/s connections. The interface carries information to enable the channels and timeslots allocated to the mobile equipments. The messaging required within the network to enable handover is also carried over this interface.

(iii) **O interface :** The RSS is connected with OSS by **O interface**. O interface uses the **Signaling system No. 7 (SS7)** based on X.25 and carries management data to/from the RSS.

Other interfaces that are used in GSM are :

(i) **B interface :** B interface exist between the MSC and the VLR. It uses a protocol known as the **MAP/B protocol**. We know that most VLRs are collocated with an MSC. This makes the interface purely an "internal" interface. The interface is used whenever the MSC needs to communicate with the VLR in order to access data regarding an MS located in its area.

(ii) **C interface :** The C interface is used to provide communication between the HLR and a GMSC. The call that is originating from outside the network has to pass through the gateway so that routing information required to complete the call may be gained. This interface uses **MAP/C protocol.**

(iii) **D interface :** The VLR and the HLR communicates via D interface. It uses the **MAP/D** protocol. The information related to the location of MS is exchanged between the VLR and HLR over this interface.

(iv) **E interface :** The E interface provides communication between two MSCs. It uses **MAP/E** protocol to exchange data related to handover between the anchor and relay MSC.

2.1.5 GSM Protocols and Signaling Architecture

MU - May 14

Q. Explain the GSM protocol architecture. **(May 14, 10 Marks)**

- Fig. 2.1.4 presents the protocol architecture of GSM with signaling protocols and interfaces.

Based on the interface, the GSM signaling protocol is assembled into three general layers :

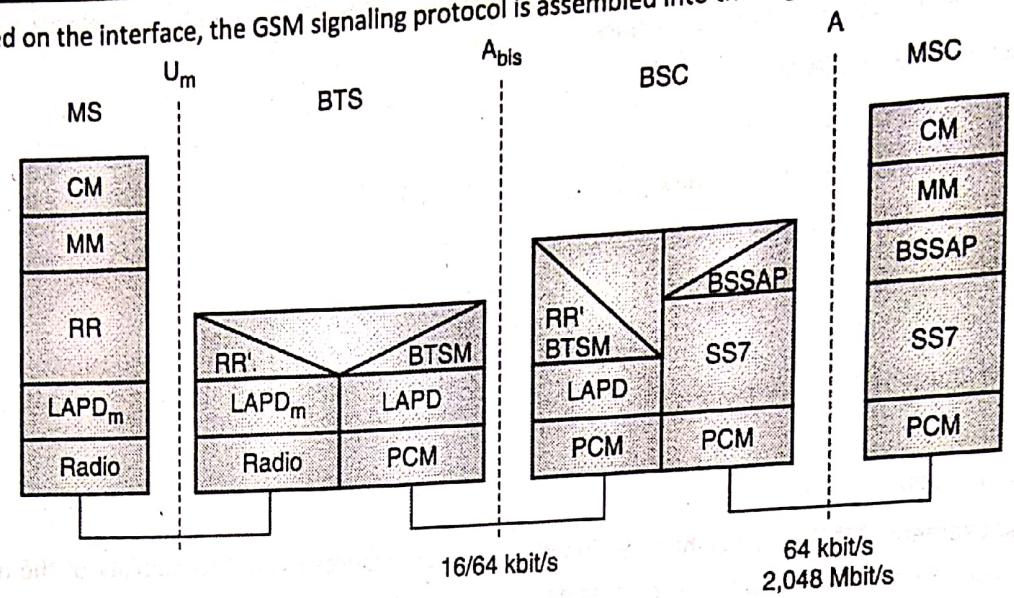

Fig. 2.1.4 : GSM protocol stack for signaling

Layer 1 : The physical layer, which uses the channel structures over the air interface.

- The main functions of physical layer are :
  - Handles all radio-specific functions
  - Creation of bursts
  - Multiplexing of bursts into TDMA frames
  - Synchronization with the BTS
  - Detection of idle channels
  - Measurement of the channel quality on downlink.
- The physical layer at U_m interface uses GMSK for digital modulation and performs encryption/decryption of data.

Layer 2 : The data-link layer

- The data-link layer uses LAPDm (Link access protocol on the D_m channel) protocol across the Um interface,
- LAPD (Link access protocol for the D channel) is the ISDN protocol for D channel.
- $LAPD_m$ is a modified version of LAPD for mobile stations. It does not need synchronization flags or check sum for error detection.
- $LAPD_m$ offers following functionality :
  - Reliable data transfer over connections
  - Re-sequencing of data frames
  - Flow control
  - Segmentation and reassembly of data
  - Acknowledged/unacknowledged data transfer.

Layer 3 : The third layer of the GSM signaling protocol is divided into three sub layers:

- Radio Resource management (RR)
- Mobility Management (MM) and
- Connection Management (CM).

The MS to BTS Protocols

- The RR layer takes care of 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 and is configuring the radio channels.
- The **MM layer** is built on top of the RR layer and handles the functions that arise from the mobility of the subscriber. It also handles authentication and security aspects.
- The **CM layer** is responsible for call control (CC), supplementary service management, and Short Message Service (SMS) management. Each of these may be considered as a separate sub layer within the CM layer.

BSC Protocols

- After the information is passed from the BTS to the BSC, the A_{bis} interface is used between the BTS and the 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** 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 to MSC, the relay is using SS7 protocols and the BSS mobile application part (BSSAP) is used to communicate from the BSC to MSC.

MSC Protocols

- At the MSC, the information is mapped across the A interface.
- Here the equivalent set of radio resources is now called the BSS Application Part (BSSAP).
- This completes the relay process. Through the control-signaling network, all 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.

Signaling system No. 7 (SS7)

SS7 is used for signaling between MSC and a BSC. This protocol is used to transfer all management information between MSCs, HLR,VLRs, AuC, EIR, and OMC.

2.1.6 Localization and Calling Description of the Call Setup Procedure

GSM supports automatic, worldwide localization of users. The system always knows location of the user, and the same phone number is valid worldwide. As soon as mobile station moves to a new area, its VLR change. The HLR sends all user data needed to the new VLR.

To locate mobile station and to address the MS, several numbers are needed :

1. **Mobile Station International ISDN Number (MSISDN)**
   - This is the mobile phone number of the user.
   - This number consists of the **country code (CC)** followed by national **destination code** (NDC) (address of service provider) and the **subscriber number (SN)** (e.g. +91 973 1234567).

2. **International Mobile Subscriber Identity (IMSI)**
   - GSM uses IMSI for internal unique identification of a subscriber.
   - IMSI consists of a mobile country code (MCC), the mobile network code (MNC) (the code of service provider), and the mobile subscriber identity number (MSIN).
3. **Temporary Mobile Subscriber Identity (TMSI)**
   - To hide the IMSI over radio interface, GSM uses 4 byte TMSI for local subscriber identification.
   - TMSI is selected by the current VLR and is valid for temporarily and within the location area of the VLR.
   - VLR may change TMSI periodically.
4. **Mobile Station Roaming Number (MSRN)**
   - MSRN is a temporary address generated by VLR that is used to hide the identity and location of a subscriber.
   - The VLR generates this address on request from the MSC.
   - This MSRN address is also stored in the HLR.
   - MSRN contains the current **Visitor Country Code (VCC)**, the identification of the **current MSC** and the **subscriber number**.
   - All these above mentioned numbers are needed to locate a mobile station and maintain connection with it.

2.1.6(a) Initialization

- Whenever a mobile station (MS) is powered on, sequence of operations have to be performed in order to activate the mobile in the given network.
- First, MS looks for the carrier on which the broadcast channel is transmitted.
- In order to do this, MS scans all 124 channels and measures their received power level. The carrier containing the broadcast channel is emitted at a much higher power than other carriers in the same cell.
- The MS lists the measured carriers according to their decreasing power.
- In the next step, the MS listens to the subsequent carriers from the list and searches for the frequency correction channel (FCCH). This is done by scanning 0^{th} slot of the broadcast carrier.
- The MS carrier frequency is then adjusted to that frequency.
- MS then finds other important control information by scanning 0^{th} slot of subsequent frames.
- At this moment the passive part of the MS activation in the network is completed.

2.1.6(b) Registration and Location Update

- In order to initiate a call or to be paged, MS has to register itself with the network.
- Registration takes place if the Location Area Identity (LAI) number received by the MS from the BTS is different than what is stored in the MS.
- The location update takes place in following cases:
  - When the MS has been switched off and wants to become active, or
  - When it is active but not involved in a call, and it moves from one location area to another.
  - After a regular time interval.
- The **Location Update process** consists of the following phases :
  1. Request for service
  2. Authentication
  3. Ciphering
  4. Update HLR/VLR
  5. TMSI re-allocation

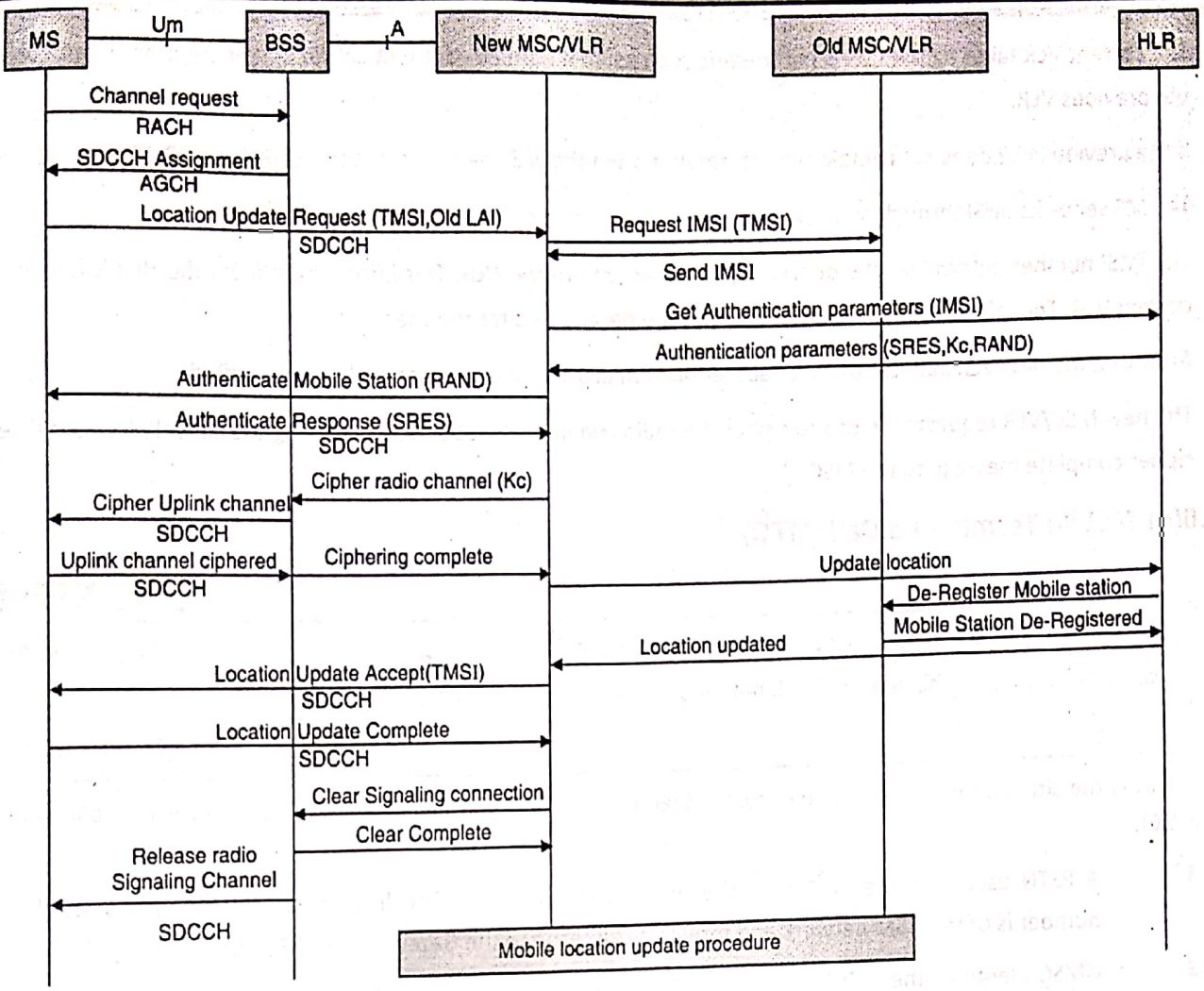

Fig. 2.1.5 : Registration and location update

- At this point, we are ready to inform the HLR that the MS is under control of a new VLR and that the MS can be de-registered from the old VLR. The location of the user is updated in the HLR.
- The new LAI and TMSI is sent to the MS. MS confirms the new LAI and TMSI. Here the location update procedure is complete. The SDCCH channel is released.
- The step by step procedure is illustrated in Fig. 2.1.5.
- The first task an MS has to do is to acquire a channel for registration. The MS does this by transmitting the RACH in which the MS requests the BTS for a channel to be used for registration.
- The BTS transfers this request to the BSC.
- In turn the BSC informs the BTS to assign a free Standalone Dedicated Control Channel (SDCCH) to the MS.
- The BTS sends the confirmation to MS on Access grant channel (AGCH) and allocates SDCCH to MS.
- In turn the MS sends the location update request on newly assigned SDCCH. The request contains TMSI and old LAI.
- This request is forwarded to the new MSC and corresponding VLR through the BTS and BSC.
- If the VLR already contains the user's TMSI, it updates its data.
- If no TMSI exist for that user then the LAI sent by the user is decoded. The LAI indirectly describes the VLR that previously served the MS.

- The current VLR takes all the user's parameters such as IMSI number, authentication and encryption parameters from the previous VLR.
- If the previous VLR does not contain this information then the MS needs to transmit its IMSI on SDCCH.
- The MS sends its IMSI through air only once. This happens at the first entry to the network.
- The IMSI number determines the ***address of the user data in the HLR***. This information from the HLR is loaded in the current VLR. The information contains authentication parameters for the user.
- After that the new VLR initiates the user authentication process and the user replies are verified.
- The new MSC/VLR requests the BSS to cipher the radio channel. The BSS upon ciphering the downlink channel sends a cipher complete message to the MSC.

2.1.6(c) Mobile Terminated Call (MTC)

MU - May 14, Dec. 15

Q. Describe the call initiation and call termination procedure in GSM systems. **(May 14, 10 Marks)**

Q. Explain Mobile Call termination in GSM, detailing the need and the use of MSRN, IMSI, TMSI nos. **(Dec. 15, 10 Marks)**

This is the situation where a terminal from a fixed network calls a mobile station. This involves the following steps (Fig. 2.1.6).

Step 1 : A PSTN user dials the phone number of a GSM subscriber. The fixed network (PSTN) notices that the number is of the GSM network and forwards call setup to the Gateway MSC (GMSC).

Step 2 : GMSC identifies the HLR (from the IMSI number of the called MS) for the subscriber and signals the call setup to the HLR.

Step 3 : The HLR now checks whether the number exists and whether the user has subscribed to the requested service.

Step 4 : HLR requests a Mobile subscriber roaming number (MSRN) from the current VLR.

Step 5 : HLR receives MSRN. And the HLR can determine responsible MSC for the MS.

Step 6 : The HLR forwards this information to GMSC.

Step 7 : The GMSC forwards call setup request to the MSC.

Step 8, 9 : The MSC first requests the current status of the MS from the VLR.

Step 10 : If the MS is available, the MSC initiates paging in all cells.

Step 11 : The BTSs of all BSSs transmit this paging signal to the MS.

Step 12, 13 : The MS answers.

Step 14, 15 : The VLR does security checks.

Step 16, 17 : The Connection is setup.

Fig. 2.1.7 illustrates the messages exchange between the MS and the BTS taken place during the connection setup.

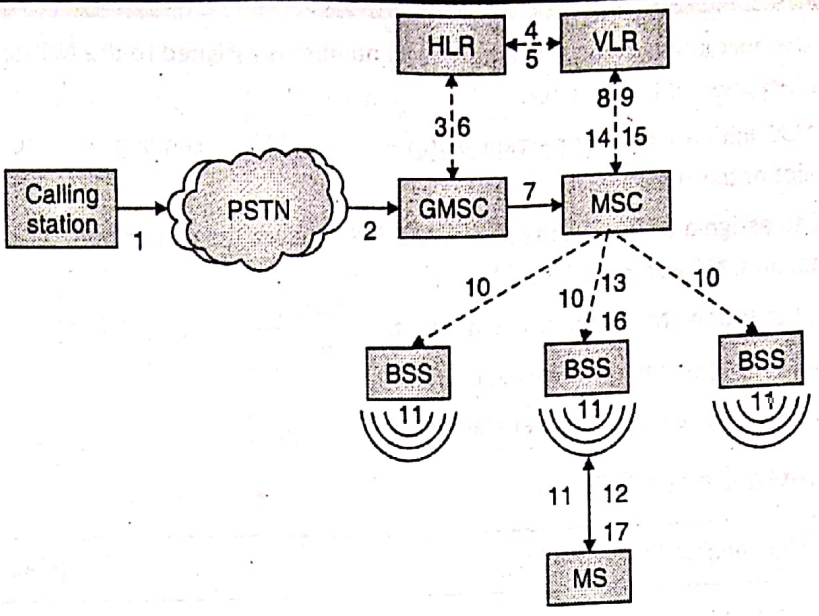

Fig. 2.1.6 : Mobile terminated call

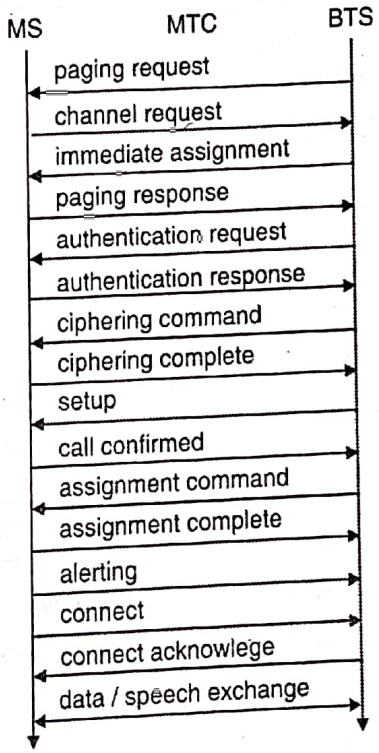

Fig. 2.1.7 : Message flow for MTC

- Note that the location area is served by many base stations. So after determining this area, the MSC sends a paging request to all BSCs operating in the determined location area.
- If the mobile station detects the paging directed to it, it requests the BTS for the channel on RACH.
- The BSC then assigns the SDCCH channel to the MS and informs MSC about the assignment.
- MS sends the paging response on this assigned SDCCH.
- Now VLR initiates the MS **authentication** process that involves the MSC, BSC an MS.
- After the MS has been authenticated, the VLR issues a command to MSC to start **data encryption**. The MSC in turn transfers this command to the MS through BSC and BTS.

- After the initiation of the encryption in the MS, a new TMSI number is assigned to the MS for the time of connection. The MS acknowledges reception of this number.
- At this moment the MSC initiates the **connection setup** with the MS by sending a set up message to it. The MS acknowledges the receipt of this message.
- MSC then informs BSC to assign a traffic channel to the MS. MS receives the carrier number, a time slot and a training sequence for the connection. MS acknowledges these parameters.
- The MS then starts ringing and the MSC is informed about it.
- The MSC then sends the ringing signal to the calling user.
- After the MS accepts the call, actual data transfer starts.

MU - May 16, Dec. 16

2.1.6(d) Mobile Originated Call (MOC)

Q. Explain how Mobile Originated Call (MOC) work. **(May 16, Dec. 16, 10 Marks)**

It is much simpler to perform a mobile originated call (MOC) compared to MTC. This follows the following steps (Refer Fig. 2.1.8).

Step 1 : The MS transmits the request for a new connection. This is realized by the MS sending a random access burst on RACH logical channel.

Step 2 : The BSS forwards this request to the MSC.

Step 3, 4 : MSC then checks if this user is allowed to setup a call with the requested service.

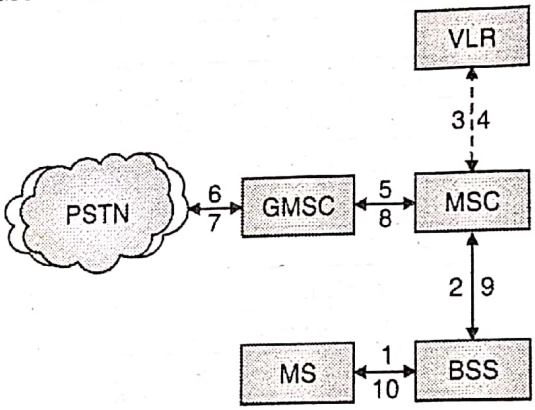

Fig. 2.1.8 : Mobile originated call

Step 5-8 : The MSC checks the availability of resources through GSM network and into the PSTN.

Step 9, 10 : If all resources are available, the MSC sets up a connection between MS and the fixed network.

In addition to the above steps, other messages are exchanged between an MS and BTS during connection setup. Fig. 2.1.9 shows the messages for MOC.

- MS has to receive an access grant on AGCH in response to the channel request sent on RACH. This AGCH contains the number of the SDCCH assigned to the MS to be used for connection set up.
- All subsequent communication between the MS and the BTS will happen on this assigned SDCCH.
- The MS sends call set up request to the BSC via BTS.
- The BSC transfers this message to the MSC.
- MSC in turn informs the VLR associated with it about the call set up request issued by the MS.

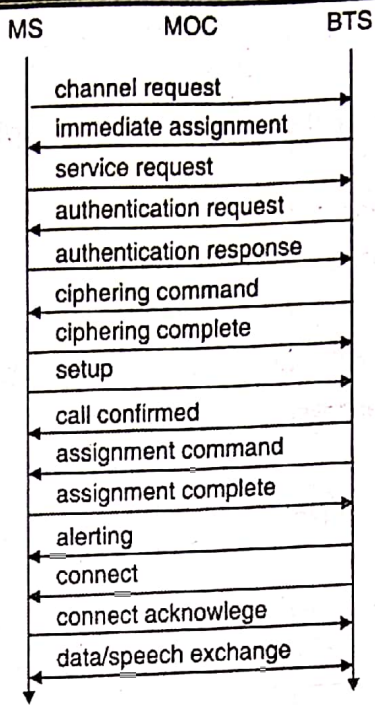

Fig. 2.1.9 : Message flow for MOC

- In turn VLR initiates authentication process.
- After the MS has been authenticated, the encryption procedure is started by the VLR.
- A new TMSI number is assigned to the MS. The MS acknowledges the reception of TMSI. The MSC then assigns a fixed link to the call and a traffic channel to the MS.
- MS acknowledges the channel assignment. This information reaches the MSC.
- MSC sends the alert message to the MS through BSC and BTS when the called mobile station starts ringing.
- When the called mobile station accepts the call, the MS is informed about it by sending connect message.
- Finally MS acknowledges this connect message and data transfer starts.

2.1.7 Handover in GSM

MU - May 15, May 16

Q. Explain various types of handoffs in GSM network. **(May 15, 5 Marks)**

Q. What are the different types of handover in GSM ?Explain in detail intra-MSC handover ? **(May 16, 10 Marks)**

- When a mobile user is engaged in conversation, the MS is connected to the BTS via radio link. If the mobile user moves to the coverage area of another BTS, the radio link to the old BTS is eventually disconnected, and a radio link to the new BTS is established to continue the conversation. This process is called handover or handoff.
- Handover is required in cellular networks, as a single base station do not cover the whole service area.
- The number of handovers to be performed depends on two factors :
  - **Cell size :** The smaller is the size of cell more the handovers required.
  - **Speed of MS :** Higher the speed of MS more handovers are required.

There are two basic reasons for handover :

1. **MS moves out of the range of BTS**
   - As a mobile station is moved out of the range of BTS, the received signal level falls below the minimal requirement of communication.
   - The error rate grows due to interference and low signal strength.
   - All these effects may diminish the quality of radio link and make communication impossible.
2. **Load balancing**
   - If the traffic in one cell is too high then the MSC or BSC shifts some MS to other cells.
   - Fig. 2.1.10 shows the four possible handover scenarios in GSM.

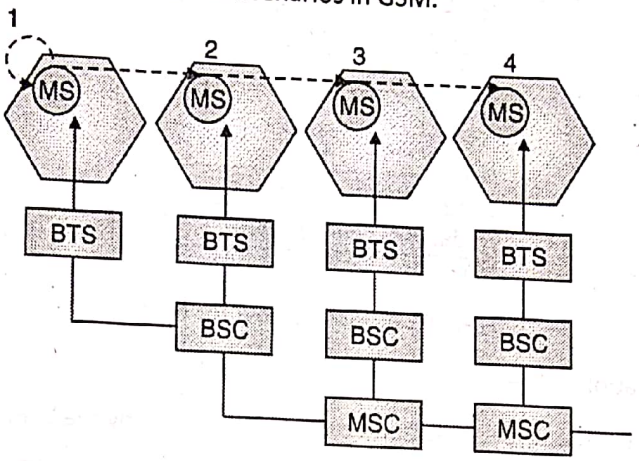

Fig. 2.1.10 : Handover scenario in GSM

(i) **Intra-cell handover :** This handover takes place within a cell. This handover is performed in order to optimize the traffic load in the cell or to improve the quality of the connection by changing the carrier frequency (scenario 1).

(ii) **Inter-cell, intra-BSC handover :** This handover occurs when a mobile station moves from one cell to another cell, but stays within the control of same BSC. The BSC then performs the handover, it assigns a new radio channel in the new cell and releases old one (scenario 2).

(iii) **Inter-BSC, intra-MSC handover :** This handover takes place between two cells managed by different BSCs. This handover is controlled by MSC (scenario 3).

(iv) **Inter MSC handover :** Inter MSC handover takes place between two cells belonging to different MSCs. Both MSCs perform the handover together (scenario 4).

Inter-BSC, Intra-MSC handover

- Fig. 2.1.11 shows the typical signal flow during an inter-BSC, intra-MSC handover.
- The MS sends its periodic measurement reports to the BTS_{old}.
- The BTS_{old} forwards these reports to the BSC_{old} together with its own measurements.
- Based on these values the BSC_{old} decides to perform a handover and sends the message HO_required to the MSC.
- The MSC then requests the resources needed for the handover from the new BSC.
- This BSC_{new} checks, if enough resources are available. If the resources are available then it activates a physical channel at the BTS_{new} for the MS.
- BTS_{new} sends acknowledgement of successful channel activation to BSC_{new}. and BSC_{new} acknowledges the handover request.
- The MSC then issues a handover command that is forwarded to the MS.

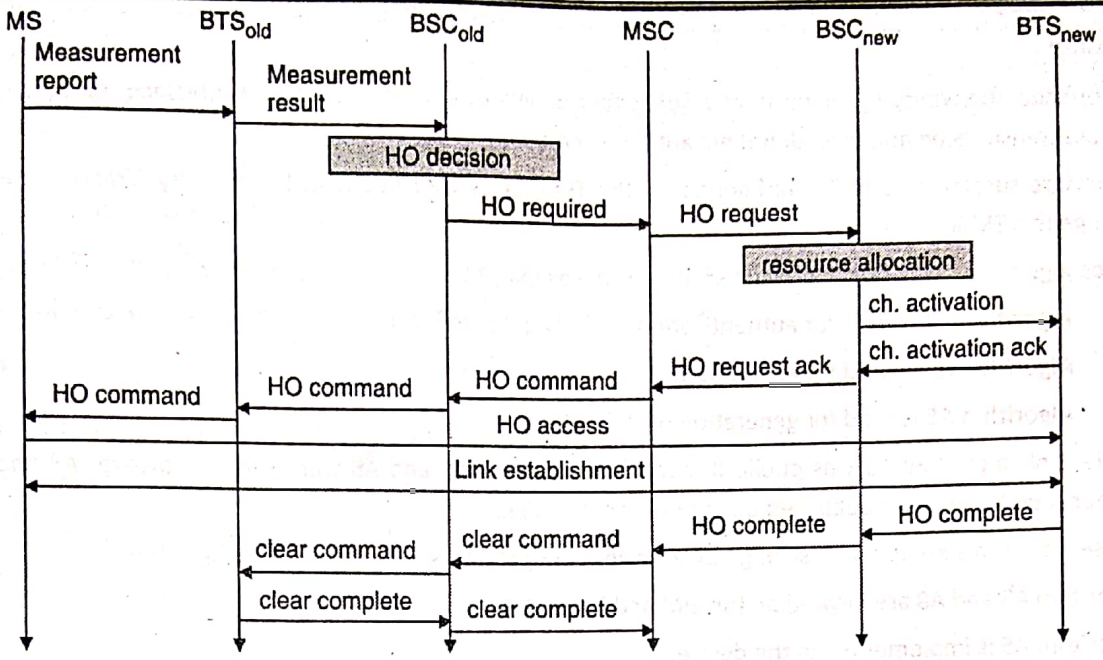

Fig. 2.1.11 : Intra MSC, inter BSC Handover process

- The MS now breaks the old connection and accesses the new BTS. Now a new radio link is established between the MS and BTS$_{new}$.
- All the reserved resources at the old BSC and BTS are released.
- Note that in the GSM systems the measurements are performed by both MS and the BTS.
- The quality and the power level of the received signal are measured in both the directions. The MS performs regular measurements of the 16 strongest carriers transmitting the BCCH.
- The measurements of the six best carriers are transmitted to the BTS every 0.48 sec.

2.1.8 GSM Security

MU - May 12, Dec. 14, May 15, Dec. 16

Q. What are the functions of Authentication and Encryption in GSM ? **(May 12, 10 Marks)**

Q. Describe how data encryption is done is GSM system, with diagram explaining the role of SIM, A3, A5 and A8 algorithm. **(Dec. 14, 10 Marks)**

Q. Write a short note on Privacy and authentication in GSM. **(May 15, 10 Marks)**

Q. Explain in detail how Subscriber Authentication is done GSM. **(Dec. 16, 10 Marks)**

GSM offers several security services using confidential information stored in the **AuC** and the **SIM**. These security services offered by GSM are explained as follows.

1. Access control and authentication

- This includes the authentication of a valid user for the SIM. The user needs to enter a secret PIN to access a SIM.
- The GSM network also authenticates the subscriber. This is done through the use of a challenge-response mechanism.

2. Confidentiality

- In GSM, confidentiality of user data is achieved by encrypting the data over air interface.
- After authentication MS and BTS apply encryption to voice, data, and signaling information.
- The confidentiality exists between MS and BTS only. It does not exist end-to-end.

3. Anonymity

- To provide anonymity the identity of a subscriber is always hidden over the air interface. All data is encrypted before transmission and user identifiers are not used over the air.
- To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. VLR may change this TMSI at any time.
- Three algorithms are used to provide security services in GSM.
  - **Algorithm A3** is used for authentication.
  - **Algorithm A5** is used for encryption.
  - **Algorithm A8** is used for generation of cipher key.
- Earlier only algorithm A5 was publically available, where as A3 and A8 were secret. However A3 and A8 are no longer secret they were published on the Internet in 1998.
- These algorithms are not very strong however network providers can use stronger algorithms.
- Algorithm A3 and A8 are located on the SIM and in the AuC.
- Algorithm A5 is implemented in the device.
- Hence algorithm A3 and A8 can differ but algorithm A5 is common for all service providers.

Authentication

- Before accessing any GSM service the user must be authenticated.
- Authentication is based on SIM that stores the individual **authentication key Ki, the user identification IMSI** and the **algorithm A3.**
- Authentication process uses challenge-response method.

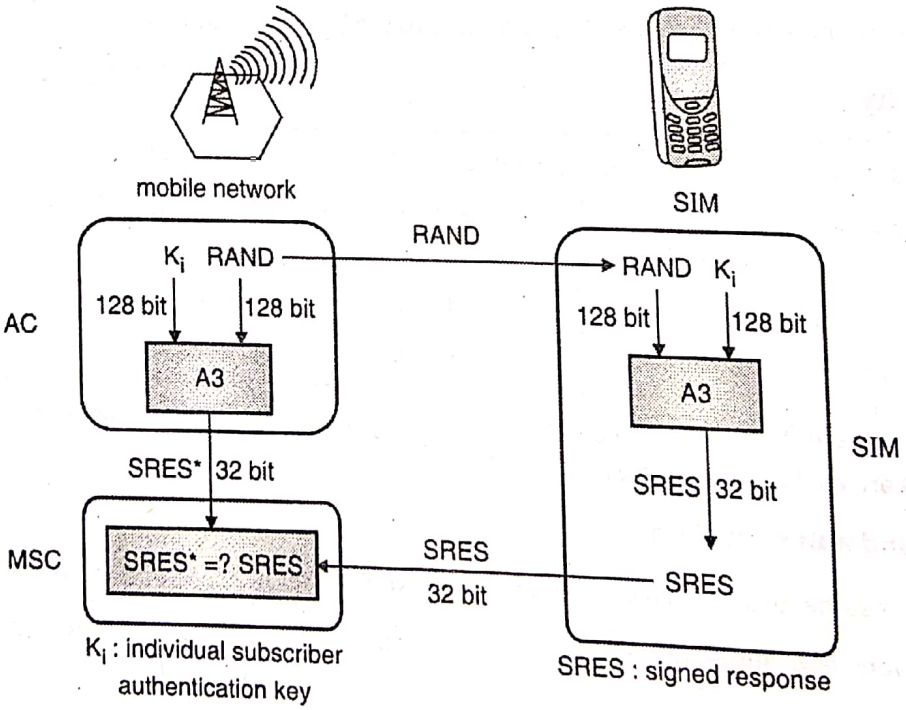

Fig. 2.1.12 : Authentication in GSM

- Steps involved in authentication process are illustrated in Fig. 2.1.12.
  1. The access control (AC) generates a 128 bit random number RAND as challenge.
  2. VLR sends this 128-bit random number (RAND) to the MS.

3. The MS computes the 32-bit signed response (SRES) based on the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki).
4. MS sends this SRES to the MSC.
5. Similarly, access control also calculates the signed response called SRES.
6. Now MSC compares the values of signed response received by AC and MS. If the values are same then the subscriber is accepted, otherwise subscriber is rejected.

Encryption

To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.

- Once authentication is done, MS and BSS can initiate encryption.
- Steps involved in Encryption process are described in Fig. 2.1.13.

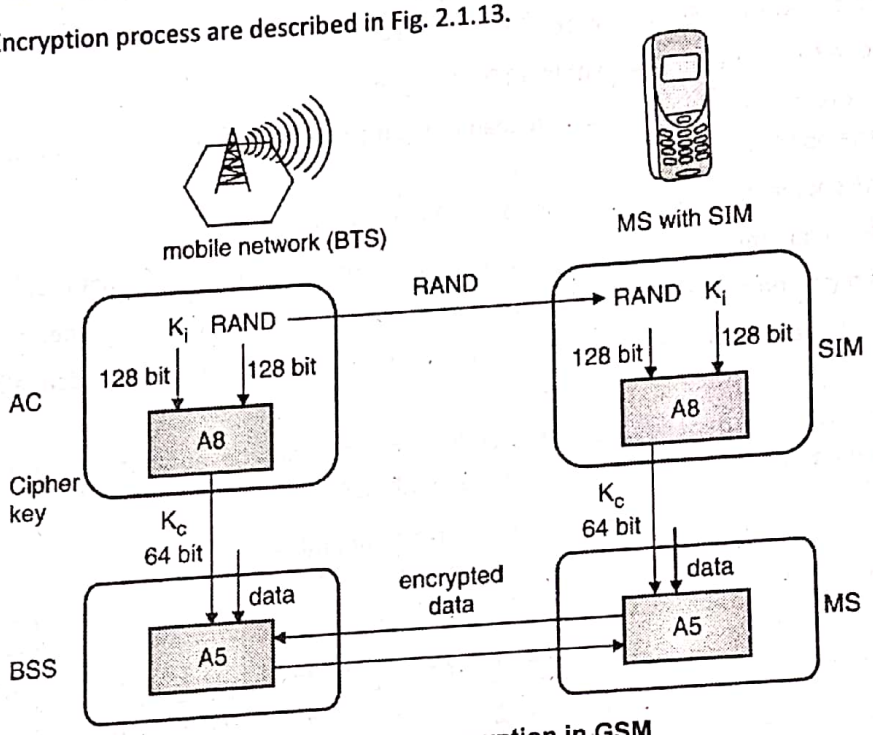

Fig. 2.1.13 : Data encryption in GSM

- The SIM and access control (AC) generate the 64 bit **cipher key Kc** by using the authentication key K_i and 128 bit random number RAND and applying algorithm A8.
- The MS and BTS can now encrypt and decrypt data using algorithm A5 and the cipher key K_c.
- The K_c which is 64 bit is not very strong but just enough to provide protection against simple eavesdropping.
- In certain implementations it so happen that 10 out of 64 bits are always set to 0, so that the real length of the key now is only 54. Hence the encryption is much weaker.

2.2 General Packet Radio System (GPRS)

MU - May 12, Dec. 12, Dec. 13, Dec. 14

Q. How much of the original GSM network does GPRS need? Which elements of the network perform the data transfer? **(May 12, 5 Marks)** **(Dec. 12, 5 Marks)**

Q. Short note on GPRS.

Q. Which components are new in GPRS as compared to GSM ? What is their purpose? **(Dec. 13, 10 Marks)**

Q. What are the modifications require to an existing GSM network to be upgraded to GPRS ? Explain with the help of diagram. **(Dec. 14, 10 Marks)**

- General Packet Radio System (GPRS) standard was defined by European Telecommunications standards Institute (ETSI).
- It is a major improvement and extension to the standard GSM system.
- GSM is a circuit-switched network which is ideal for the delivery of voice but not suitable for transmitting data that is bursty and asymmetric in nature.
- GPRS added packet-switched functionality to existing networks as a result the users of the system can be online, allowing to make voice calls and access internet on-the-go.
- GPRS uses unused time slots of GSM system to transmit packet data.
- GPRS can allocate one to eight time slots within a TDMA frame.
- Allocation of time slots is an on demand basis instead of fixed and predetermined. This allocation depends on current network load and the operator preference.
- Depending upon the coding, the transfer rate up to **171.2 kbits/s** is possible.
- GPRS operators offer a minimum of one time slot per cell to ensure at least minimum data rate.
- Charging in GPRS is based on the volume of data exchanged and not on the connection time.
- GPRS also includes several security services such as authentication, access control, confidentiality of user identity and user data.
- The available user data rate depends upon the coding scheme and the number of TDMA time slots allocated. Table 2.1.3 lists the data rates available in GPRS if it used with GSM.

Table 2.1.3 : GPRS data rates

Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

Key Features of GPRS

1. **Always online feature :** Since GPRS uses packet switched network, it removes the dial-up process. Users now can be online all the time.
2. **An upgrade to existing systems :** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
3. **Volume based charging :** In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent. With packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time.
4. **An integral part of future 3G systems :** GPRS is the packet data core network for 3G systems EDGE and WCDMA.

2.2.1 Architecture

MU - May 12, May 13, Dec. 13, Dec. 14, May 15, May 16, Dec. 16

Q. Draw and explain architecture of GPRS network. **(May 12, 5 Marks)**

Q. Draw a neat diagram of GPRS system architecture and explain with different types of interfaces. **(May 13, 10 Marks)**

Q. Which components are new in GPRS as compared to GSM ? What is their purpose ? **(Dec. 13, 10 Marks)**

Q. What are the modifications required by an existing GSM network to be upgraded to GPRS ? Explain with the help of diagram. **(Dec. 14, May 16, Dec. 16, 10 Marks)**

Q. Explain GPRS architecture in detail. Compare it with GSM architecture. **(May 15, 10 Marks)**

Fig. 2.2.1 shows simplified GPRS network architecture. As stated earlier, GPRS is an extension to traditional GSM system.

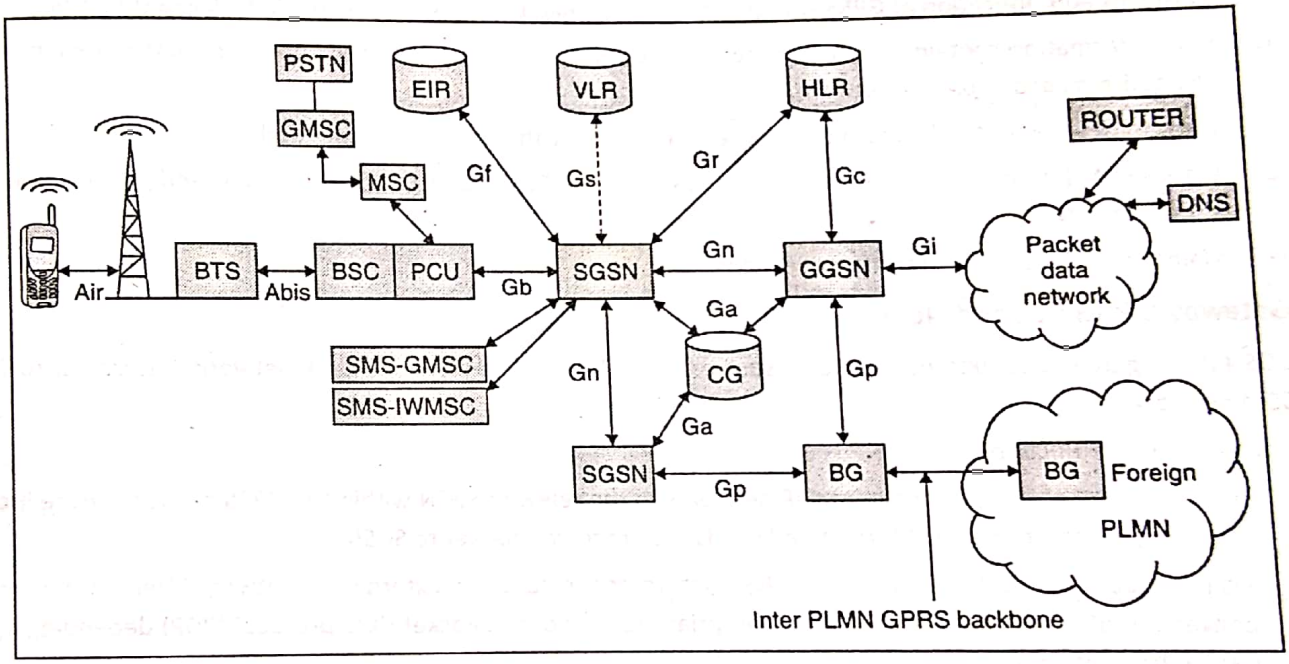

Fig. 2.2.1 : GPRS Network architecture

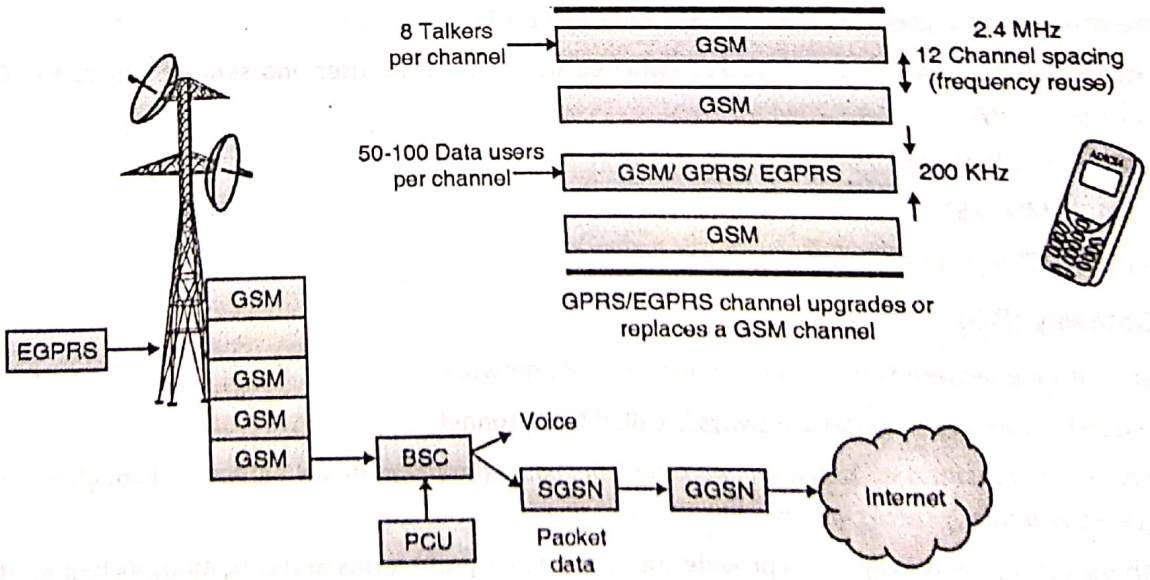

Fig. 2.2.2 : Upgrading GSM to GPRS Diagram

The following network nodes have been added to the existing GSM network to support packet switched network.

1. GPRS Support Nodes (GSNs)

- The most important network node added to the GSM network is GSN (GPRS Support Node).
- It is a network node which supports the use of GPRS in the GSM core network. All GSNs should have a *Gn* interface and support the GPRS tunneling protocol (GTP). There are two key variants of the GSN, namely serving and gateway GPRS support node.

2. Serving GPRS Support Node (SGSN)

- It is similar to MSC of GSM network. SGSN functions are listed below.
  - Performs data compression which helps to minimize the size of transmitted data units.
  - Performs authentication of GPRS subscribers and also maintains information of all the GPRS subscribers.
  - Such information contains the current cell, the current VLR and a subscriber's profile consisting IMSI number and the address used in packet network.
  - Determines the route of transmitted packets and transfer them to appropriate nodes.
  - Manages MS mobility as the subscriber moves from one PLMN area to another PLMN, and possibly one SGSN to another SGSN.
  - Maintains the statistics of traffic collections.

3. Gateway GPRS Support Node (GGSN)

- GGSN is the gateway to external networks such as PDN (Packet Data Network) or IP network. It is similar to GMSC of GSM network.
- It does two main functions.
  - Routes packet coming from external IP networks to the relevant SGSN within the GPRS network. Here it converts incoming packet to the GSM format and sends the processed packet to SGSN.
  - Routes packets originated from a GPRS user to the respective external IP network. Here it performs the conversion of the GPRS packet to the appropriate format of the Packet data protocol (PDP) depending upon the destination network.

4. Packet Control Unit (PCU)

- PCU is the core unit to segregate between GSM and GPRS traffic.
- It separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively.
- In GPRS, PCU has following two paths.
  (i) PCU-MSC-GMSC-PSTN
  (ii) PCU-SGSN-GGSN-Internet (packet data network)

5. Border Gateway (BG)

- It acts as an interface between different operators of GPRS networks.
- The connection between two border gateways is called GPRS tunnel.
- It is more secure to transfer data between two operators using their own PLMN networks through a direct connection rather than via the public Internet which is less secure.
- For this both operators need to agree to provide such connectivity and terms and conditions including charging terms.

6. Charging Gateway (CG)

- Charging gateway is responsible for accounting and billing for the use of the network.
- Charging is done based on Quality of Service or plan user has opted.
- This charging data generated by all the SGSNs and GGSNs in the network is referred to as Charging Data Records (CDRs).
- The Charging Gateway (CG) collects all of these CDRs, processes the same and passes it on to the Billing System.

7. DNS server

It converts domain name to IP addresses required to establish internet connection and to deliver web pages on user's terminal screen.

8. PLMN

(i) Intra PLMN

An IP based network inter-connecting all the above mentioned GPRS network elements in one PLMN area.

(ii) Inter PLMN

Inter PLMN is a connection between two different PLMN areas.

9. HLR Register

HLR stores information and the user profile of all GPRS subscribers. The data includes the current SGSN and PDP addresses. These data are updated each time a user registers with a new SGSN.

10. SMS-GMSC and SMS-IWMSC

- The GPRS system allows SMS messages to be sent as well. For that data exchange between SMS-GMSC and
- SMS-IWMSC blocks and the appropriate SGSN takes place.

11. GPRS Interfaces

Different interfaces have been defined between different network components of the GPRS. Some new interfaces to GSM have been added in GPRS to support packet switched data mainly between GGSNs, SGSNs and other network components. The following interfaces have been defined.

(i) **Um interface :** Between MS and BTS there is an **Um** interface which is very similar to GSM and defines the modulation type, error correction/detection technique, power control information etc.

(ii) **A interface :** BTS and BSC communicates via A interface and defines the channel allocation, power measurement information etc.

(iii) **Gb interface :** It connects BSCs to SGSN.

(iv) **Gn interface :** Gn interface exist between GSNs of same PLMN. It is used to exchange user profile when the user moves from one SGSN to another.

(v) **Gp interface :** Two GSNs of different PLMN communicate via Gp interface. It is used for exchanging the user profile and other signaling information between a SGSN and GGSN of another area.

(vi) **Gf interface :** It is used between SGSN and EIR. It is used to query the IMEI information if an MS tries to register with the network.

(vii) **Gr interface :** SGSN and HLR communicate via **Gr** interface. It is used to get the user profile, the current SGSN address and the PDP address(es) for each user in PLMN.

(viii) **Gc interface :** Between GGSN and HLR there is **Gc** interface. It is used by GGSN to query user's location and profile to update its location register.

(ix) **Gi interface :** Connects GGSN to external PDN.

(x) Gs interface : Between SGSN and MSC/VLR is used to perform paging request of circuit switched GSM call for combined attachment procedure.

(xi) Gd interface : Between SMS-Gateway (SMS-GMSC) and SGSN is used to exchange short message service (SMS) messages.

(xii) GPRS Tunneling protocol (GTP) : All GSNs forming a GPRS backbone network are connected over IP. Within this backbone the GSNs encapsulate and transmit PDN packets by using GPRS Tunneling Protocol (GTP).

2.2.2 GPRS Protocol Stack

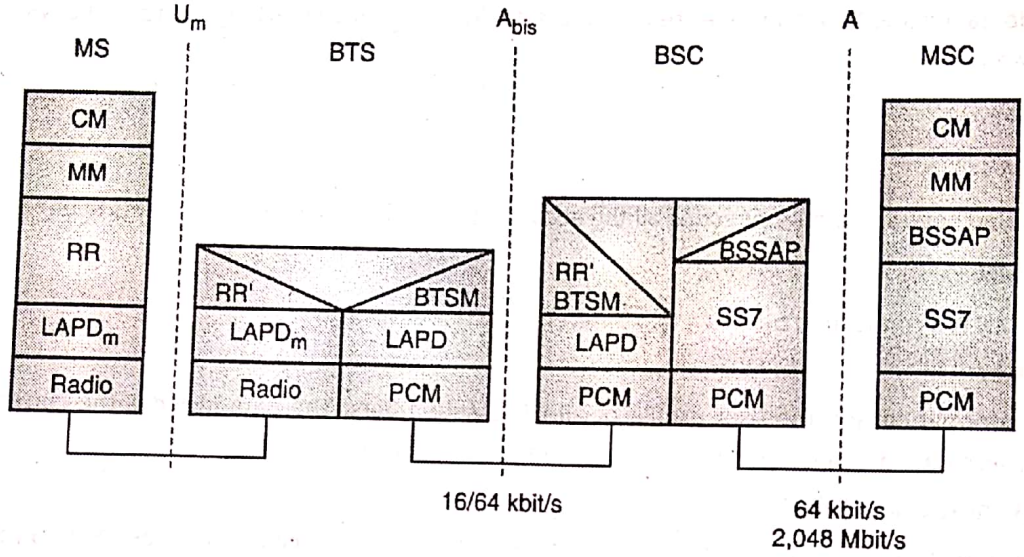

Fig. 2.2.3 : GPRS protocol architecture

The following various protocols are involved in GPRS :

1. **GPRS tunneling protocol (GTP)**

   It is responsible for all the data transfer between GSNs.

2. **TCP/UDP**

- Depending on the requirement, GTP can use either TCP or UDP as the transport layer protocol.
- UDP is used in case non-reliable data transfer is required (IP packet transfer).
- TCP is used in case reliable data transfer is required (X.25 packet transfer).

3. **Subnetwork dependent convergence protocol (SNDCP)**

- It is used between the SGSN and the MS to adapt to the characteristics of the underlying networks.
- User data packet is tunneled between the MS and the GGSN on top of SNDCP and GTP.

4. **Logical link control**

- It is used to provide reliable data transfer between the MS and the SGSN.
- It comprises ARQ and FEC mechanism for PTP (Point-To-Point) services.

5. **Base station subsystem GPRS protocol (BSSGP)**

- This protocol is used to convey routing and QoS-related information between the BSS and SGSN.
- It works on the top of a frame relay (FR).

6. **Radio link protocol (RLC)**

   It is responsible for providing a reliable link between the MS and the BSS.

7. **Medium access control (MAC)**
   - It is responsible for controlling the medium access and the signaling procedure for the radio channel.
   - Performs mapping of the LLC frames onto the GSM physical channels.

2.2.3 Comparison of GPRS Architecture with GSM Architecture

- The existing GSM nodes are upgraded with GPRS functionality.
- The GSM network only provides circuit switched services and thus two new network nodes GSN (GPRS Support Nodes) nodes were defined to support packet switched services. They are GGSN and SGSN.
- GPRS uses GSM's BSS but with enhanced functionality to support GPRS. The GSMs BSS now is used for both circuit switched and packet switched network elements to ensure backward compatibility.
- Additional PCU (Packet control Unit) unit has been added to BSC to segregate voice and data packets.
- Circuit switched data are sent to **A** interface on the MSC and packet switched data are sent to the SGSN into the GPRS backbone.
- The BSC of GSM is given new functionality for mobility management for handling GPRS paging. The new traffic and signaling interface form the SGSN is now terminated in the BSC.
- GPRS uses the MSC/VLR interface provided by GSM, between the MSC and SGSN coordinated signaling for mobile stations which have both circuit switched and packet switched capabilities.
- The HLR of GSM is modified to contain GPRS subscription data and routing information and is accessible from the SGSN. It also maps each subscriber to one or more GGSNs. The HLR may be in a different PLMN than the current SGSN for roaming terminals

Advantages of GPRS

- Very flexible.
- Suitable for bursty Internet traffic and fully packet oriented.
- Better quality of data services measured in terms of reliability, response time.
- No connection is required to be set up prior to data transfer.
- All GPRS services can be used in parallel to the conventional GSM services.
- Users of GPRS benefit from shorter access times and higher data rates.
- GPRS packet transmission offers a more user friendly billing than that offered by circuit switched services.

Disadvantages of GPRS

- The real available data rate depends on the current load of the cell as GPRS only uses idle time slots.
- Additional network elements are required to implement GPRS.
- GPRS exhibits a large jitter as compared to fixed networks.

Application of GPRS

1. **Communications :** E-mail, fax, unified messaging and intranet/Internet access etc.
2. **Value-added services :** Information services and games etc.
3. **E-commerce :** Retail, ticket purchasing, banking and financial trading etc.
4. **Location-based applications :** Navigation, traffic conditions, airline/rail schedules and location finder etc.
5. **Vertical applications :** Freight delivery, fleet management and sales-force automation.
6. **Advertising :** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

7. **SMS :** It is also possible to send SMS messages over GPRS.
8. **Supplementary services :** GPRS also offers supplementary services, such as call forwarding and closed user group (CUG).

2.3 UMTS Terrestrial Radio Active Network (UTRAN)

2.3.1 UMTS (Universal Mobile Telecommunication System) Core Network

- Universal Mobile Telecommunication System (UMTS) is the European proposal for IMT-2000 prepared by ETSI.
- The UMTS specifically defines new radio interface called UMTS Terrestrial Radio Interface (UTRA).
- Two radio interfaces have been defined: UTRA-FDD and UTRA-TDD.
- UMTS does not define a complete new 3G system rather it specifies a smooth transition from second generation GSM or TDMA systems to the third generation.
- Many solutions have been proposed for 3G networks.
- One initial enhancement of GSM towards UMTS was Enhanced Data rates for Global Evolution (EDGE) which uses enhanced modulation techniques.

UMTS services

UMTS should provide following services as a 3G network :

1. Provide various bearer services.
2. Support real-time and non real-time services.
3. Support Circuit switched and packet switched transmission.
4. Handover should possible between UMTS cells, but also between other non-UMTS systems such as GSM or satellite networks.
5. The system should be compatible with GSM, ATM, IP and ISDN-based networks.
6. Should provide variable data rates for uplink and down link.

2.3.2 UMTS System Architecture

Q. Write a short note on UMTS architecture and its domain. **MU - May 12, May 15**

Q. Explain UMTS architecture. **(May 12, 5 Marks) (May 15, 5 Marks)**

- Fig. 2.3.1 shows the simplified UMTS reference architecture.

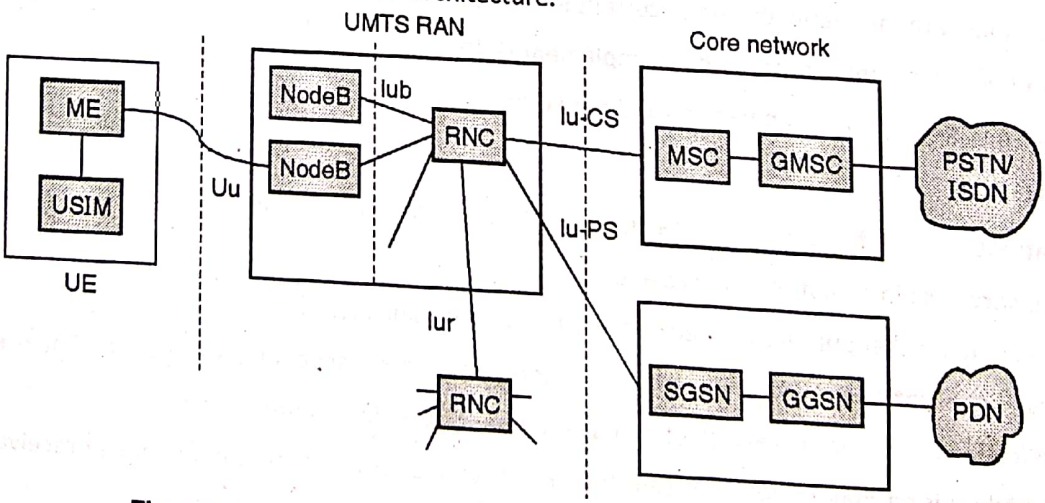

Fig. 2.3.1 : Main components of the UMTS reference architecture

Three main components of UMTS are :

1. The UTRA network (UTRAN)
2. Core Network (CN)
3. User Equipment (UE)

1. UTRAN

- The UMTS Terrestrial network (UTRAN) handles the cell level mobility and comprises several radio network subsystems (RNS).
- RNS consists of two main components: RNC(Radio Network Controller) and Node B.
- Node B is similar to the base station in GSM system, which performs physical layer processing such as channel coding, modulation, data interleaving etc.
- RNC controls one or more Node Bs. It manages radio resources assigned to them. Thus it performs data link layer processing and also participates in handover process.
- RNC is connected to MSC and SGSN to route circuit switched and packet switched data.
- In general the functions of RNS includes :
  - Radio channel ciphering and deciphering
  - Handover control
  - Radio resource management
  - Admission control
  - Congestion control
  - System information broadcasting
  - Radio network configuration etc.
- UTRAN is connected to Users Equipment via the radio interface Uu. Uu interface is comparable to Um interface in GSM.
- UTRAN communicates with the Core Network (CN) via Iu interface which is similar to the A interface in GSM.

(i) Core Network (CN)

- Core network is shared with GSM and GPRS.
- It contains components such as HLR, VLR, MSC , GMSC , SGSN and GGSN.
- Core network contains functions for inter-system handover, gateways to other networks, and performs location management.

(ii) User Equipment (UE)

- The user equipment (UE) contains two components: Mobile equipment (ME) and UMTS subscriber Identity Module (USIM).
- ME is the radio terminal connecting to the radio interface using Uu interface.
- USIM is a smart card similar to SIM in GSM system that contains the subscriber identity, authentication algorithms, encryption keys etc.
- UMTS further subdivides the above architecture into two domains as shown in Fig. 2.3.2.

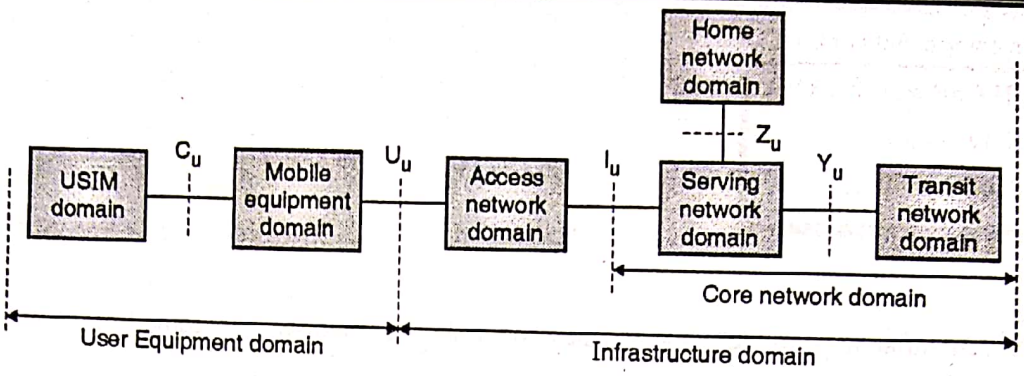

Fig. 2.3.2 : UMTS domain and interfaces

The user equipment domain

- The user equipment domain is assigned to a single user and comprises all the components needed to access UMTS services.
- The end device itself is in a mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.
- This domain is further divided into two sub domains: The **USIM domain** and **mobile equipment domain.**
- The USIM domain contains the SIM for UMTS and stores all the necessary user related data. It also performs functions for encryption and authentication of users.

The infrastructure domain

- The infrastructure domain is shared among all the users.
- It offers UMTS services to all the subscribed users.
- It is further divided into two sub domains. The **access networks domain** and the **core network domain.**
- Access network domain contains the radio access networks (RAN) and provides radio access to the UMTS users.
- Core network domain contains functions that are independent of access network.
- The core network domain can be separated into three domains with specific tasks.
  - The serving network domain
  - The home network domain
  - The transit network domain
- The **serving network domain** comprises all functions currently used by a user for accessing UMTS services.
- The **Home network domain** contains all functions related to the home network of a user for example, user data look-up, user profile.
- If the serving network cannot directly contact the home network then **transit network domain** may be used.

UMTS radio interface

- The UMTS defines a new radio interface *Uu* between the user equipment and the UTRA network.
- The UMTS uses direct sequence (DS) CDMA technology.
- In DS-CDMA each user is separated using a special code called chipping sequence.
- It multiplies a stream of bits with a chipping sequence to spreads the signal.
- To separate different users the codes the codes that are used for spreading should be orthogonal.
- All signals use the same frequency band. UMTS uses the constant chipping rate of 3.84 Mchips/s.
- Different data rates can be achieved by using different spreading factors. Spreading factor is defined as the number of chips per bit.

- Fig. 2.3.3 shows basic idea of spreading and separation of user data using orthogonal spreading codes.
- The first step is spreading the user data using orthogonal spreading codes.

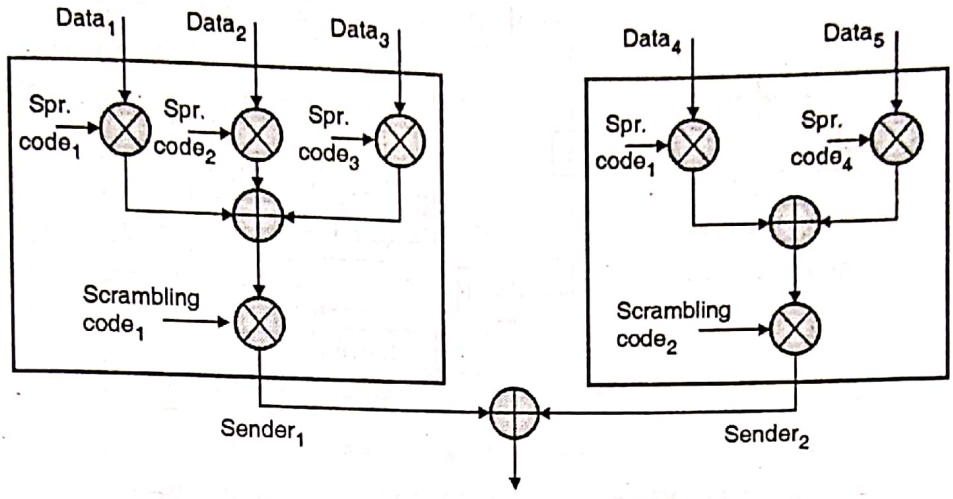

Fig. 2.3.3 : Spreading and scrambling of user data

- UMTS uses orthogonal variable spreading factor (OVSF) codes.

Working of OVSF

- Orthogonal codes are generated by doubling a chipping sequence X with and without flipping the sign of the chip.
- For example if a chipping sequence is X the next set of orthogonal codes would be (X,X) and (X,-X) as shown in Fig. 2.3.4 (a).

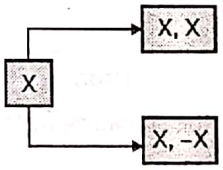

Fig. 2.3.4 (a) : Generation of orthogonal codes

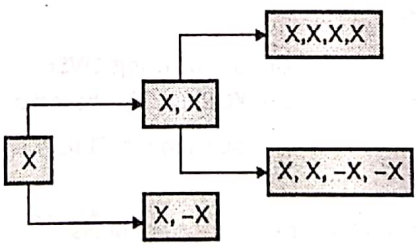

Fig. 2.3.4 (b) : Generation of orthogonal codes

- Now chipping sequence XX is doubled without flipping the signs and with flipping the signs. We get two more sets (X,X,X,X) and (X,X,-X,-X) (Fig. 2.3.4 (b)).
- The whole process of generating OVSF codes is shown in Fig. 2.3.5 assuming the starting chipping sequence as 1.

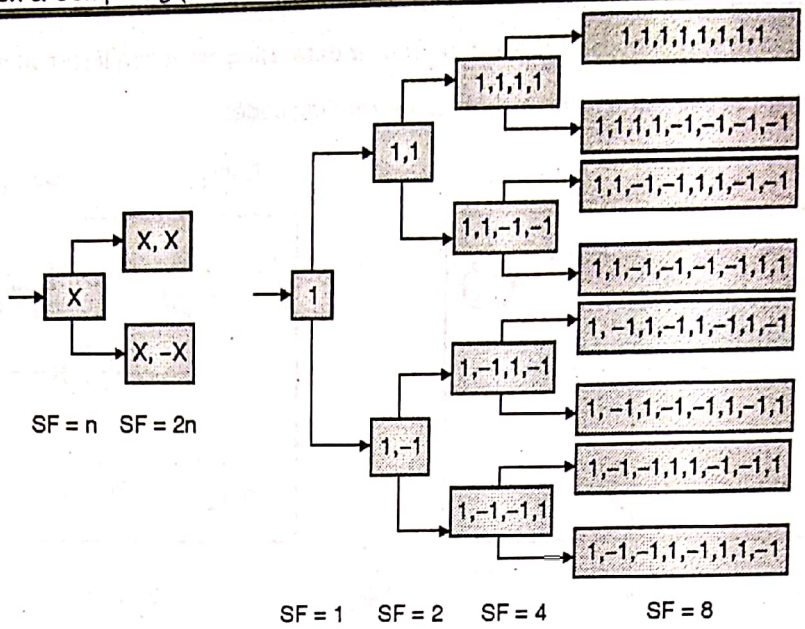

Fig. 2.3.5 : OVSF code tree used for orthogonal spreading

- Doubling the chipping sequence also results in spreading the bit twice as much as before. The spreading factor SF=n becomes SF=2n.
- Two codes are orthogonal as long as one code is not the part of another code. Thus orthogonality can be guaranteed if one code is not generated from the other code.
- Thus if a sender uses the code (1,–1) with spreading factor as 2, it is not allowed to use any of the codes located in the sub tree generated out of (1,–1).

Supporting different data rates

- UMTS uses constant chipping rate of 3.84Mchip/s.
- Different data rates are achieved by varying spreading factor.
- If the chipping rate is constant and if we double the spreading factor this will result in spreading the bit twice as much as before. Thus, it divides the data rate by two.
- Thus, by using different spreading factors we can achieve different data rates.

Spreading and scrambling of user data

- As shown in Fig. 2.3.3 each user spreads its data stream using OVSF code. After spreading, all chip streams are summed up and scrambled. Scrambling is nothing but XORing chips based on a code.
- In the FDD mode, the scrambling code is unique for each sender. Thus, here scrambling code is used to separates all senders in a cell.
- After scrambling the signals of different senders are quazi-orthogonals.
- For TDD the scrambling code is cell specific i.e. all the stations in a cell use the same scrambling code.
- The scrambled chips are then modulated using QPSK and then transmitted.

2.3.2(a) UTRA – FDD (W-CDMA)

MU - May 13, May 15

Q. Explain UTRA FDD in detail. **(May 13, May 15, 5 Marks)**

- The FDD mode for UTRA uses wideband CDMA (W-CDMA) with direct sequence spreading.
- In FDD, uplink and downlink uses different frequencies.

Features of W-CDMA

- 1920-1980 MHz uplink
- 2110-2170 MHz downlink
- Uses constant chipping rate of 3.840 Mchip/s
- Provides soft handover
- Uses QPSK for modulation
- Requires complex power control (1500 power control cycles/s)
- Spreading : Up Link : 4-256;Down Link:4-512

UTRA-FDD Frame structure

- Fig. 2.3.6 shows UTRA-FDD frame structure.
- A radio frame contains 15 time slots. The duration of each frame is 10 msec.
- A radio frame consists of 38,400 chips.
- Each time slot is of 666.6 μs and consists of 2,560 chips.
- Each W-CDMA channel occupies 4.4 to 5 MHz bandwidth.
- Time slots in W-CDMA are not used for user separation but to support periodic functions. In contrast to GSM where time slots are used to separate users.

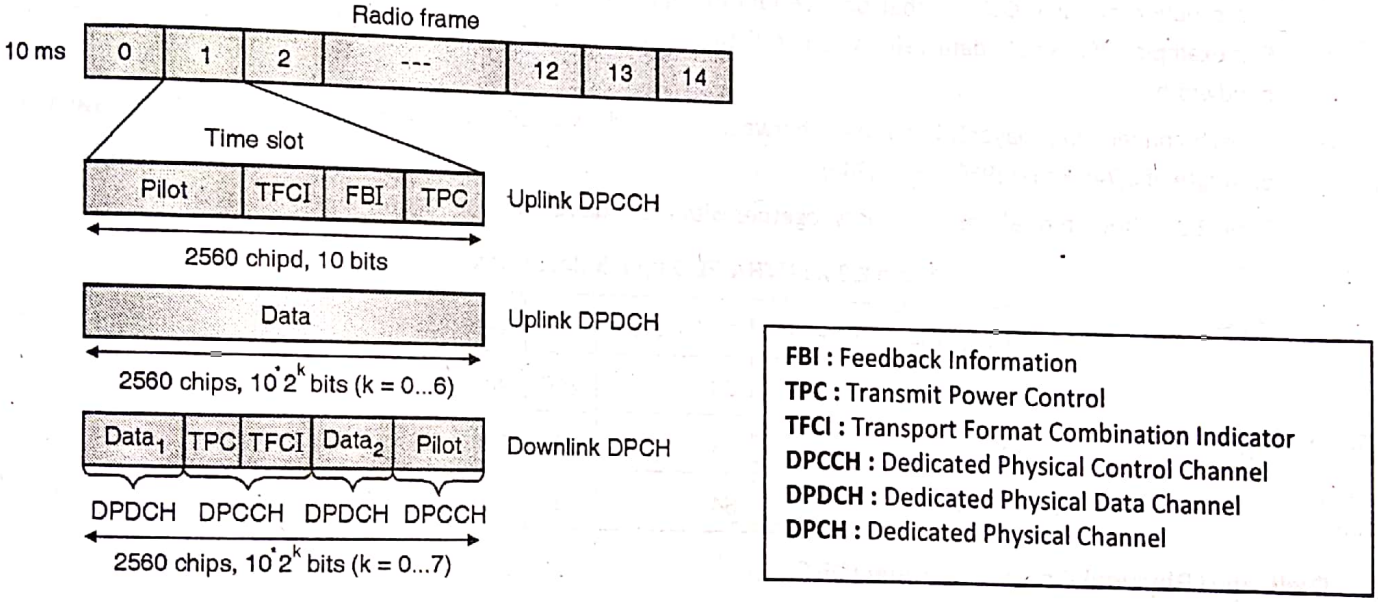

Fig. 2.3.6 : UTRA –FDD (W-CDMA) frame structure

Similar to GSM, UMTS also defines many logical and physical channels and their mapping.

Physical Channels in UMTS

- UMTS supports three physical channels which are used for data transport.
  - Dedicated Physical Data Channel (DPDCH)
  - Dedicated Physical Control Channel (DPCCH)
  - Dedicated Physical Channel (DPCH)
- And additionally a Random Access Channel (RACH) to control the media access in uplink.

1. Dedicated Physical Data Channel (DPDCH)

- This channel is used for transferring user data and signaling data.
- The spreading factor of this channel can vary between 4 and 256. This directly supports different data rates.
- Table 2.3.1 describes different spreading factors and corresponding data rate supported by DPDCH.

Table 2.3.1 : Spreading and corresponding data rates supported by DPDCH

Spreading factor	Data rate (kbits/s)
4	960
8	480
16	240
32	120
64	60
128	30
256	15

- Thus, maximum data rate supported is 960 kbit/s with spreading factor 4.
- The problem of using OSVF is that only certain multiplies of the basic data rate (i.e. 15 kbit/s) can be used. For example, 250 kbit/s data rate is required then the device has to choose 480 kbit/s, which wastes the bandwidth.
- In each connection in layer1, it can have between zero and six DPDCHs. This results in a theoretical maximum data rate of 5,740 kbit/s ($960 \times 6 = 5,740$).
- Table 2.3.2 shows typical user data rates together with the required data rates on the physical channel.

Table 2.3.2 : UTRA-FDD uplink data rates

User data rate [kbit/s]	12.2 (voice)	64	144	384
DPDCH	60	240	480	960
DPCCH	15	15	15	15
Spreading	64	16	8	4

2. Dedicated Physical Control Channel (DPCCH)

- In each connection, layer 1 needs exactly one DPCCH.
- This channel conveys control data for the physical layer.
- It uses constant spreading factor 256.
- The channel contains following four fields.

(i) **Pilot :** The pilot is used for channel estimation.

(ii) **Transport format combination identifier (TFCI) :** TFCI specifies the channel transported within the DPDCHs.

(iii) **Feedback information field (FBI) :** It supports signaling for a soft handover.

(iv) **Transmit power control (TPC) :** TPC is used for controlling the transmission power of a sender. Power control is performed in each slot, thus 1500 power control cycles are available per second. Tight power control is necessary to mitigate near-far-effects. Six different DPCCH bursts have been defined which differ in the size of the fields.

3. Dedicated Physical Channel (DPCH)

- This is downlink channel.
- It multiplexes control and user data.
- Spreading factors between 4 to 512 are available. The available data rates for data channels (DPDCH) within a DPCH are 6 (spreading factor = 512), 24, 51, 90, 210, 432, 912 and 1872 (spreading factor =4).

4. Physical Random Access Channel (RACH)

- It is used to control medium access on the uplink. UTRA-FDD defines 15 random access slots within 20ms.
- Within each access slot 16 different access preambles can be used for random access.
- Using slotted Aloha, User Equipment (UE) can access an access slot by sending a preamble.
- UE starts with the lowest available power to avoid interfering with other stations. If no positive response is received then UE tries for another slot with another preamble with the next higher power level. This is called power ramping.
- The number of available slots can be defined per cell and is transmitted via a broadcast channel to all Users.

Steps for searching a cell

A UE has to perform following steps during the search for a cell after a power on.

1. **Primary synchronization**

   A UE has to synchronize with the help of a 256 chip primary synchronization code. This code is same for all the cells and helps to synchronize with the time slot structure.

2. **Secondary synchronization**

   During this second phase, the UE receives a secondary synchronization code which defines a group of scrambling codes used in this cell. The UE is now synchronized with the frame structure.

3. **Identification of the scrambling code**

   The UE tries all scrambling codes within the group of codes to find the right code with the help of a correlator.

2.3.2(b) UTRA - TDD (TD-CDMA)

MU - May 13, May 15

Q. Explain UTRA TDD mode in detail. **(May 13, May 15, 5 Marks)**

Features of UTRA-TDD

- UTRA-TDD separates up link and down link in time domain. The Frame structure of TDD is similar to FDD.
- 15 slots with 2,560 chips per slot form a radio frame with duration of 10ms. The chipping rate is also 3.84 Mchip/s.
- The TDD frame structure can be **symmetrical** or **asymmetrical**.
- In symmetrical frame structure number of uplink and downlink slots is same.
- In asymmetrical frame structure any arbitrary combination is used.
- The system can change spreading factor between 1 to 16 to achieve desired data rate.
- Thus using the traffic burst shown in Fig. 2.3.7 data rates of 6624, 3312, 1656, 828 and 414 kbit/s can be achieved for spreading factors 1,2,4,6,8, and 16 respectively.
- Power control is easy due to tight synchronization and use of orthogonal codes. A simple power control scheme with 100-800 power control cycles/s is sufficient.

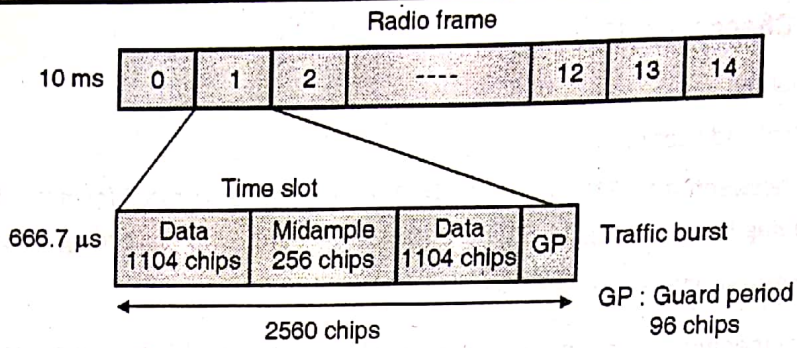

Fig. 2.3.7 : UTRA – TDD (TD- CDMA) frame structure

UTRA - TDD Frame format

- UTRA- TDD frame structure is shown in Fig. 2.3.7.
- It includes following bursts.

Data Fields

- Fig. 2.3.7 shows a burst of type2 which comprises two **data** fields each of 1,104 chips.
- Spreading is applied to these data fields only.

Midample

- Midample is used for training and channel estimation.

Guard period (GP)

- As TDD uses the same scrambling codes for all stations; the stations must be tightly synchronized and the spreading codes are available only once per slot.
- To loosen the tight synchronization little bit, a guard period has been introduced at the end of each slot.

Table 2.3.3 : Comparison of UTRA-FDD and UTRA-TDD

Parameter	UTRA-FDD	UTRA-TDD
Idea	Uses wideband CDMA (W-CDMA) with direct sequence spreading.	Uses Time domain CDMA
Separation of channels	Separates up and downlink in frequency domain	Separates up and down link in time domain.
Synchronization	Synchronization is not required in time domain	Tight synchronization is needed in time domain.
Power control	Complex power control scheme required. (1500 power control cycles/s)	Simple power control scheme is sufficient. (100-800 power control cycles/s)
Spreading	Spreading : Up Link : 4-256; Down Link :4-512	Spreading between 1-16
Maximum Data rate	960 kbit/s	6624 kbit/s
Scrambling code	Each station within a cell uses the different scrambling code.	All the stations in a cell use the same scrambling code.

2.3.3 Improvement on Core Network

- The activities of 3G developments have always focused on development of physical and MAC layers.
- The following three radio modules were selected for 3G radio access.
  (i) Direct sequence (DS) frequency division duplex(FDD)
  (ii) Multi carrier (MC) frequency division duplex (FDD)
  (iii) Time division duplex (TDD)
- The DS mode is based on the W-CDMA proposal and the MC mode is based on cdma2000 proposal. The TDD mode is basically suitable for cordless communications.
- Three major modules of core network for 3G system have been identified :
  (i) ANSI-41
  (ii) GSM MAP
  (iii) and IP-based network
- All the radio access modes of UTRAN should fully support ANSI 41 and GSM MAP.
- An operator may select one or more radio modules together with one or more core network modules to implement 3G system.
- Moreover, network related procedures are optimized to reduce signaling traffic in 3G.
- An additional improvement to the Core Network in UTRAN was addition of a new entity GLR (Gateway Location Register) between HLR and VLR.
- From the view point of VLR located in visited network, GLR is treated as roaming user's HLR in home network.
- From the view point of HLR in home network, the GLR acts as the VLR at the visited network.

Review Questions

Q. 1 Explain mobile terminated and mobile originated call in GSM.

Q. 2 Explain various security services offered by GSM.

Q. 3 Explain how the location update occurs in GSM.

□□□