2.1 Wireless Communication :

Definition :

- Wireless communication is defined as the communication by radio waves.
- The term wireless explains the communications other than the broadcast communication, between individuals who often use portable or mobile equipment.

2.1.1 Need of Wireless Communication :

- The communication systems can be classified into two broad categories as :
  1. Wired or guided communication systems.
  2. Wireless or unguided communication systems.
- The wired communication systems such as conventional telephone system use some kind of wired media such as coaxial cable or optical fiber cable to inter connect its end users.
- The **wireless systems** do not use wires as the transmission media.
- Instead air acts as the communication medium and communication takes place using electromagnetic (EM) waves.
- Examples of wireless communication systems are : Satellite communication, mobile phones, wireless LAN and WAN, etc.
- The wireless communication is needed because of the reasons mentioned below :
  1. Long distance communication is difficult using wired media due to the length of wire, maintenance problems etc.
  2. One user to multiuser communication system becomes complicated using wired media. This becomes easy with wireless links.
  3. Broadcasting applications such as radio, TV etc. are possible only through wireless communication due to a large number of users. Wired communication is not possible for such application.
  4. It is easy to add new users without any additional wiring.
  5. Wireless communication is possible even if the user is moving.
  6. Using wireless LANs or wireless communication between computer and peripherals we can avoid wiring and improve reliability.

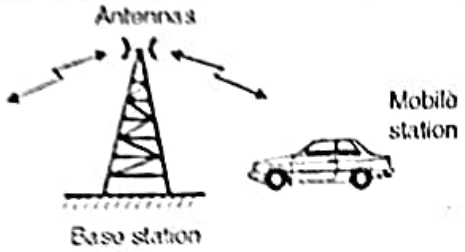
2.1.2 Wireless Communication Systems :

- Some of the wireless communication systems are as follows :
  1. Wireless LAN.
  2. Cordless telephone.
  3. Walkie-Talkie.
  4. Pagers.
  5. AC remote control.
  6. TV remote control.
  7. Cellular phones.
  8. Satellite Communication systems.
- Wireless communication is the fastest growing part of electronic communication.
- In the wireless communication systems, the signal energy propagates in the form of electromagnetic waves over the wireless media or wireless channels.
- The examples of wireless media are radio waves, microwave and infrared light.
- The wireless media does not use a conductor or wire as a communication channel. Instead it uses the air or vacuum as medium to carry the information from transmitter to receiver.
- The transmitter first converts the data signal into electromagnetic waves and transmits them using a suitable antenna.
- The receiver receives the electromagnetic waves using a receiving antenna and converts them into data signal again.

2.1.3 Important Definitions :

- Following are some of the important definitions of terms used in wireless communication systems.

1. **Base station :**
   - It is defined as a fixed (non-moving) station in a mobile radio system, which communicates with the mobile stations as shown in Fig. 2.1.1.



(G-1556) **Fig. 2.1.1 : Base station**

   - Base stations are located at the center or on the edge of a region being covered. It consists of transmitter antenna, receiver antenna and radio channels mounted on a tower.

2. **Control channel :**
   - It is defined as the radio channel used for transmitting the control signals such as call set up, call request, call initiation as well as the control information.

3. **Forward channel :**
   - It is defined as the radio channel used for transmitting the information from the base station to the mobile i.e. in the forward direction.

4. **Reverse channel :**
   - It is defined as the radio channel used for transmitting the information from a mobile to base station i.e. in the reverse direction.

5. **Mobile station :**
   - It is defined as a station in the cellular radio service which is used when in motion at an unspecified location.
   - Mobile stations can be portable hand held personal units or they can be the ones installed in vehicles.

6. **Hand-off :**
   - It is the process of transferring the connection with a mobile station from one base station to the other when the mobile station moves from the service area of one base station into that of the other.

7. **Mobile switching center (MSC or MTSO) :**
   - It is defined as the center which is set up for coordinating the routing of calls.
   - An MSC is also called as MTSO i.e. mobile telephone switching office.

8. **Transceiver :**
   - It is a unit containing transmitter as well as receiver. It can simultaneously transmit as well as receive.

9. **Page :**
   - A page is defined as a small message which is broadcast over the complete service area,in the simulcast manner, simultaneously by many base stations.

10. **Roamer :**
    - A roamer is a mobile station which operates in a service area other than the one from where the service has been subscribed.

11. **Subscriber :**
    - We may define a subscriber as a user of a mobile communication system, who pays the subscription charges.

12. **Half duplex system :**
    - A half duplex system is a bidirectional system i.e. it can transmit as well as receive but not simultaneously.
    - At a time these systems can either transmit or receive, for example a transreceiver or walky talky set.
    - The direction of communication will keep changing itself.

13. **Full duplex systems :**
    - The full duplex systems are the truly bidirectional systems which allow the communication to take place in both the directions simultaneously.
    - These systems can transmit as well as receive simultaneously, for example the telephone systems.

2.2.1 Basic Cellular System :

- Cellular telephone system is a wireless telephone system. It is a multiuser system.
- In this section we are going to study the second type of multiuser system called mobile radio system or wireless communication system.

Concept :

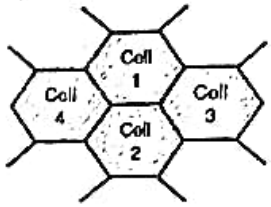
- Cellular phone is wireless communication just like cordless phone.
- In cell phone distance is not restricted to within home but one can travel in the city or even outside the city without interruption in communication.
- The demand for cellular mobile phone is increasing at alarming level and is likely that wired communication will be replaced by wireless technology.
- In the cellular system city is divided into small areas called 'cells'. Each cell is around 10 square kilometer (depends upon power of base station).

MTSO or MSC :

- The cells are normally thought of hexagons. Because cell phones and base stations use low power transmitters, the same frequencies can be reused in non-adjacent cell.
- Each cell is linked to central location called the Mobile Telephone Switching Office (MTSO). It is also called as Mobile Switching Center (MSC).
- MTSO coordinates all mobile calls between an area which consists of several cell sites and the central office.
- Time and billing information for each mobile unit is accounted for by MTSO.
- At the cell site base station is provided to transmit, receive, and switch calls to and from any mobile unit within the cell to the MTSO.
- A cell covers only few square kilometer area, thus reducing the power requirement necessary to communicate with cellular telephones.
- In this manner heavily populated areas can be serviced by several stations, rather than one as used by conventional mobile techniques.

Cell :

- The basic geographic unit of a cellular communication system is called as a **cell.**
- Its shape is hexagonal as shown in Fig. 2.2.2(a). Cells have the base stations transmitting over small geographic areas.

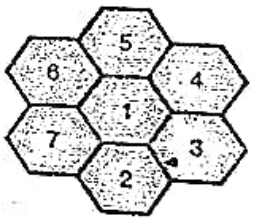


(G-1026) **Fig. 2.2.2(a) : Cell**

- The size of a cell is not fixed. Practically the shape of the cell may not be a perfect hexagon.
- The hexagonal shape has been adopted universally because it allows easy and manageable analysis of a cellular system.

Cluster :

- A group of cells is called as a **cluster.** Fig. 2.2.2(b) shows the cluster of seven cells or a seven cell cluster (n = 7).



(G-1027) **Fig. 2.2.2(b) : Cluster**

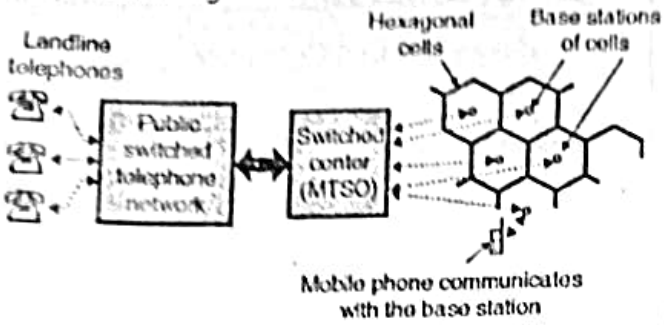
- The cluster size (n) is not fixed. It depends on the requirements of a particular area.

2.2.2 Structure of Cellular Phone System :

Block diagram :

- In the communication systems discussed so far, the transmitter and the receiver both were stationary.
- In the **mobile communication** which we are going to discuss now, either the transmitter or the receiver or both are going to be movable.
- As the points between which the communication takes place are movable, the communication channel has to be air, that means it is a wireless communication.

- The structure of the mobile phone network along with the public switched telephone networks is shown in Fig. 2.2.3.



(G-1025) **Fig. 2.2.3 : Basic structure of mobile telephone network**

- Cellular telephone system is a wireless telephone system. It is a multiuser system.

Description :

- The mobile telephone system has hexagonal shaped cells as shown in Fig. 2.2.3. Each cell has a base station situated at the center.
- The task of the **base stations** is to act as an interface between the mobile phone and the cellular radio system.
- The base stations of all the cells are connected to the switched center **MSC**. Observe that this interface is a bi-directional one.
- That means the exchange of information between the switched center and the base stations is a two way.
- As shown in Fig. 2.2.3, the communication area of the mobile communication is divided into hexagonal cells.
- Therefore, the system is named as the **cellular radio system.**
- The switching center acts as the interface between the Public Switched Telephone Network (**PSTN**).
- In addition to that it performs the supervision and control operations in the mobile communication system.
- Due to this kind of a system layout, the communication can take place between two mobile subscribers or between a mobile subscriber and a landline telephone as well.
- If a mobile subscriber travels from one cell area to the other then it automatically gets connected to base station of that cell.
- Thus the service provided to a mobile subscriber is continuous without any break.

Functions of MTSO (MSC) :

- The MTSO control all the cells and provides the interface between each cell and the main telephone office.
- As the mobile user from one cell to the next cell, the system automatically switches from one cell to the next.

  The computer at MTSO causes transmission from the mobile user to be switched from the weaker cell to the stronger cell within a very short time.

Advantages of using MTSO (MSC) :

- There are certain advantages of using MTSO over the older MTS system :

1. It operates at a much higher frequency. So more spectrum space is available and so more number of channels can be accommodated.
2. Due to MTSO, the cellular system can use the concept of frequency reuse. This will allow the cells to use the same frequency without the fear of interference.
3. And the third advantage is that the cells of different size can be accommodated in the system.

Conditions controlled by MTSO (MSC) :

- Let us discuss the important conditions/things controlled by MTSO in the mobile phone system.

1. **Control of transmitter output power :**

- The transmitter output power is not constant but it is controllable by the cell site and MTSO.
- Special control signals picked up by the receiver are sent to an automatic power control (APC) circuit.
- The APC circuit then sets the transmitter output power to one of the eight power output levels.

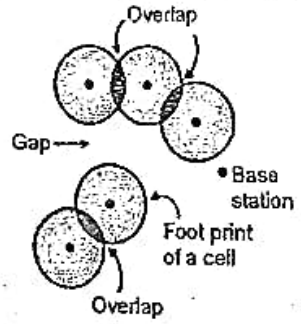
2. **Monitoring of the received signal strength :**
   - The MTSO monitors the strength of the received signal by checking the RSSI (received signal strength indicator) signal generated by the receiver.
   - Based on this signal, the MTSO makes a decision about switching to another cell.
3. **Frequency division ratio :**
   - The MTSO logic section sends the numbers corresponding to frequency division ratio.
   - These numbers are loaded into the frequency divider blocks of the frequency synthesizer.
   - This sets the transmit and receive channel frequencies.
   - With increase in the number of users or increase in the demand for service, the number of base stations can be increased.
   - The transmitter power for each base station is reduced in order to reduce the interference.
   - Thus we can increase the radio capacity without any additional radio spectrum.
   - This fundamental concept is used for all the modern wireless systems.

2.2.3 Advantages of Cellular Concept :

1. Only a fixed number of channels (frequency slots) are required to be used. This is because the same frequencies can be used for multiple cells due to the principle of frequency re-use.
2. Large area can be covered.
3. Low power transmitters can be used as the cell area is small.
4. Every piece of subscriber equipment (e.g. mobile handset) within a country or continent can be manufactured with the same set of channels so any mobile can be used anywhere.
5. Higher capacity.
6. Local interference only.
7. Robustness to failure at single component.
8. No technological challenges in deployment.

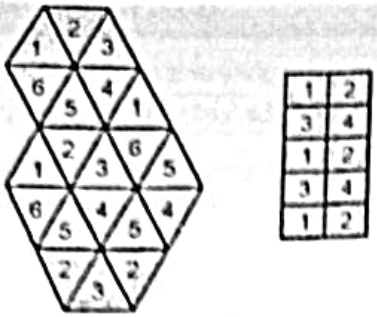
2.2.4 Hexagonal Cell Geometry :

- The signal strength decreases as it travels away from the base station.
- The coverage area of a BS is defined as the region over which the signal strength is higher than the threshold value say X dB.
- If the antenna at BS is assumed to be isotropic then the coverage area must be a circular region.
- **Footprint** is defined as the actual radio coverage of a cell.
- We can find out the footprint either from the field measurements or the propagation prediction models.
- Fig. 2.2.4 shows the footprints of different cells present in the same geographical area.

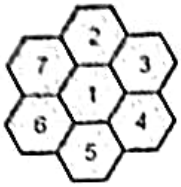


(G-2663) **Fig. 2.2.4 : Footprint of cells showing the overlaps and gaps**

- As shown in Fig. 2.2.4 there may be an overlap between the adjacent circular coverage areas or there may be a gap between the coverage areas of two adjacent cells.
- Therefore we cannot use such a circular geometry, as a regular shape to describe cells.
- It is important that for the cells of same shape in the same geographical area, there are no ambiguous areas belonging to multiple cells or to no cell.
- These requirements are satisfied if each cell is having one of the following shapes : equilateral triangle, square or regular hexagon.
- Fig. 2.2.5 demonstrates the triangular and square shapes of the cell whereas Fig. 2.2.6 shows the hexagonal cells.



(G-2660) Fig. 2.2.5 : Square and triangular cells



(G-2661) Fig. 2.2.6 : Hexagonal cells

- Out of these shapes, the hexagonal cell is the closest approximation of a circle. It is used for the cellular system.

Why hexagonal shape ?

- Following are the reasons for selecting the hexagonal shape over square or triangular cell shape :
  1. Hexagonal shape makes the analysis of a cellular system easy and manageable.
  2. The circular cell pattern allows either overlap or gaps in the adjacent cells. This is avoided if hexagonal shape is selected.
  3. A hexagon closely approximates the circular radiation pattern and provides greater coverage without creating ambiguous areas.
  4. With the hexagon used as cell geometry, we need less number of cells to cover a large area as compared to the triangular or square cell geometry.
- It is not mandatory to place the BS always at the center of the cell. If the BS is at the center of a cell then it is called as a center-excited cell.
- Sometimes the directional antennas are placed in corner excited cell for better coverage at the edges of the cell whereas the omni-directional antennas are used in centre excited cells.

2.3 Frequency Reuse :

Concept :

- In frequency reuse concept the radio channels use the same frequency to cover different areas that are physically separate from each other.
- In frequency reuse it is necessary to see that the co-channel interference is not objectionable.
- Frequency reuse is an important concept because in this a single transmitter of higher power need not be used to cover the entire area.
- Instead many transmitter of small output power operating at the same frequency can be used.
- This technique also reduces the minimum height of the transmitting antenna, because now each antenna has to cover a small area.
- Frequency reuse is very important concept of the cellular mobile radio system.
- The users located in different geographical areas i.e. different cells can use the same frequency simultaneously.
- The advantage of frequency reuse is that it drastically increases the spectrum efficiency but the disadvantage is that if the system is not designed properly then co-channel interference may take place.

2.3.1 Advantages of Frequency Reuse :

1. A single transmitter of high power need not be used to cover the entire area.
2. Many transmitter of small power working at the same frequency can be used.
3. This technique reduces the minimum height of the antenna.
4. The users located in different geographical areas i.e. different cells can use the same frequency simultaneously.
5. It drastically increases the spectrum efficiency.

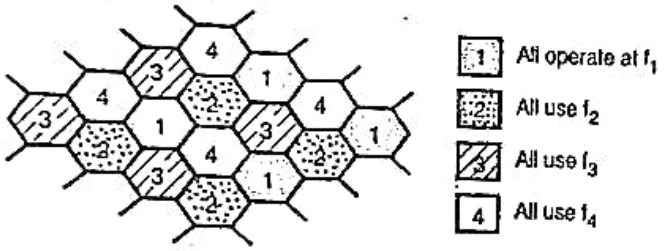
2.3.2 Frequency Reuse Schemes :

- We can use the concept of frequency reuse in either time domain or in the space domain.

- In the time domain the same frequency is used by different users in different time slots. This is called as time division multiplexing (TDM).

Frequency reuse patterns :

- There are two categories of frequency reuse in the space domain as follows :
  1. Same frequency is assigned in two different geographical areas. (Such as two different cities.)
  2. To use the same frequency repeatedly in a same general area in one system. This scheme is popularly used in cellular systems.
- The second scheme is illustrated in Fig. 2.3.1. The total available frequency spectrum is divided into 4 co-channel cell groups in the system as shown in Fig. 2.3.1.



(G-1031) **Fig. 2.3.1 : Frequency reuse**

- The cells marked-1 will use the same frequency say f_1, the cells marked-2 will use same frequency f_2 and so on.

Frequency reuse ratio :

- It is defined as 1/N where N is the cluster size. It is 1/N because each cell within a cluster is assigned only 1/N of the total available channels (frequencies) in the system.

2.4 HandOff / Handover :

Definition :

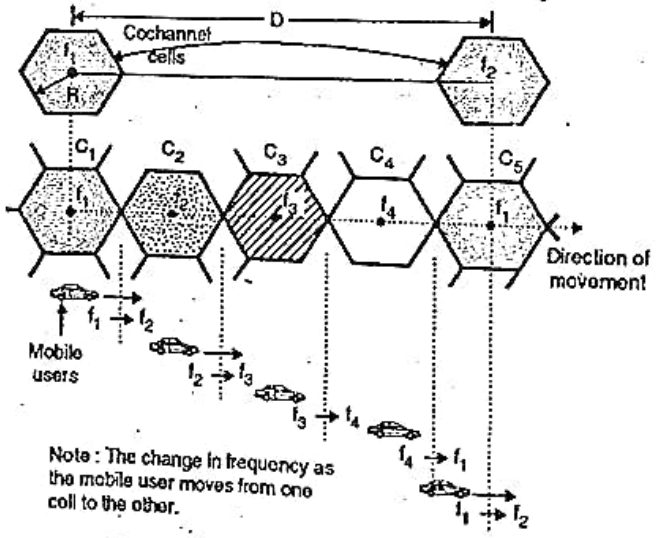
- The call in progress will continue even when the mobile station moves from one cell to the other.
- This process of continuing the call in progress without terminating it is called as **"hand-off"**.
- It is also called as **handover.**

Need of hand-offs :

- Assume that there is a call going on between two parties over a voice channel.
- When the mobile unit moves out of coverage area of a particular cell site, the reception becomes weak.
- Then the present cell site will request a handoff.
- The system will switch the call to a new cell site without interrupting the call. This procedure is called as the hand off procedure or handover procedure.
- The user can continue talking without even noticing that the handoff procedure has taken place.
- The advantage of handoff procedure is increase in the effectiveness of the mobile system.

Explanation :

- Refer Fig. 2.4.1 to understand the handoff procedure clearly.
- Fig. 2.4.1 shows two co-channel cells separated by a distance D and using the frequency f_1.
- Other cells such as C_1, C_2, C_3, C_4, C_5 etc. exist in-between the two co-channel using frequency f_1.
- The cells C_1, C_2, C_3 and C_4 use different frequencies f_1, f_2, f_3, f_4, etc. as shown in Fig. 2.4.1.



(G-1033) **Fig. 2.4.1 : Hand off procedure**

- Suppose a mobile unit initiates a call in cell C_1 and then moves to cell C_2.
- Then as it starts going away from C_1, the call is dropped and reinitiated in the frequency channel from f_1 to f_2 when the mobile unit (such as car) moves form C_1 to C_2.

- Similarly when the mobile unit moves from cell C_2 to C_3 the frequency is changed automatically from f_2 to f_3 as shown in Fig. 2.4.1.
- The process of changing the frequency is done automatically by the system and the user does not even notice it.

2.4.1 Handoff Strategies :

- It is important to process handoffs in any cellular system.
- In many hand off strategies, higher priority is given to the hand off request than the call initiation request.
- Handoffs should be performed successfully and they should not be repeated frequently.
- So as to satisfy these requirements, system designers should decide and specify an optimum signal level at which the handoff should be initiated.
- Fig. 2.4.1 illustrates handoff diagrammatically.

Handoff threshold :

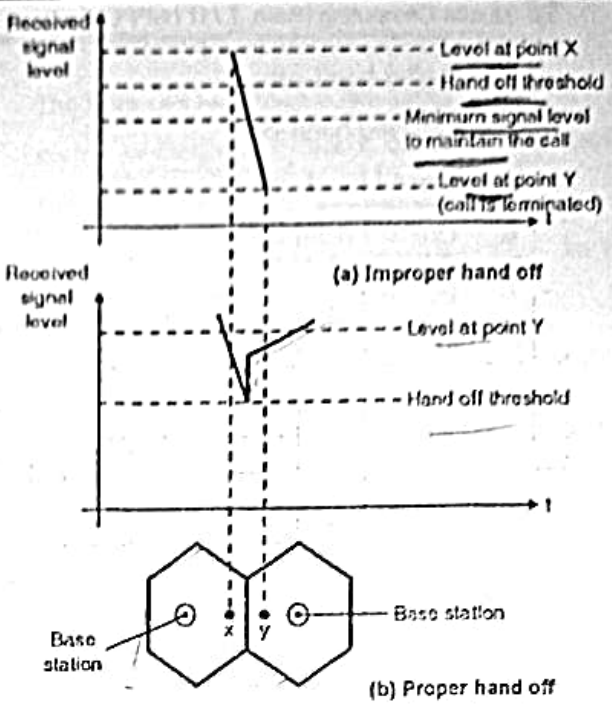
- First a minimum signal level for maintaining the call is decided.
- Then a slightly stronger signal level is used as the **handoff threshold.**
- The handoff will be made at this signal level.
- The margin between these two levels is denoted by Δ and given by,

$$\Delta = P_{r\ \text{hand off}} - P_{r\ \text{minimum usable}} \quad ...(2.4.1)$$

- Note the choice of the value of Δ is critical. Δ can not be too small and it cannot be too large as well.
- If Δ is too large, then unnecessary handoffs will take place and if Δ is too small, there won't be sufficient time to complete the handoff and the call may lost due to weak signal.

Improper handoff :

- Refer Fig. 2.4.2(a) which illustrates the **improper handoff** situation i.e. handoff is not made and signal drops below the minimum signal level. The call is terminated.



(G-1564) **Fig. 2.4.2 : Illustration of improper and proper hand off**

- In Fig. 2.4.2(b), the handoff has taken place as soon as the received signal level drops to the hand off threshold.
- Note the increase in the signal level at point Y after handoff.
- Before initiating the handoff, it is necessary to ensure that the reduction in the measured signal level is not due to the momentary signal fading and that the drop in signal level is due to the actual movement of the mobile station.

2.4.2 Dwell time :

- The time duration over which a call may be maintained within a cell without initiating a handoff is called as dwell time.
- The dwell time depends on propagation, interference, distance between the subscriber and base station etc.

2.4.3 Different Types of HandOffs :

- Following are various types of handoffs, in relation with a mobile station (MS) :
  1. Hard hand-off
  2. Soft hand-off

3. Softer hand-off
4. Delayed hand-off
5. Forced hand-off
6. Queued hand-off
7. MAHO
8. Inter cell hand-off
9. Intra cell hand-off

1. Hard hand off :

- The hand off is known as hard handoff if a mobile station transmits between two base stations operating on different frequencies.
- It means that all the old radio links in the MS are removed before the new radio links are established.
- It is generally used in GSM. We can say that it is a Break before Make strategy. Hence in this case higher rates of call drops is found.
- When mobile (in Call) switches to a new sector/Cell which is on different frequency, then it performs hard Handover.
- It is basically an inter-frequency handover.

2. Soft hand off :

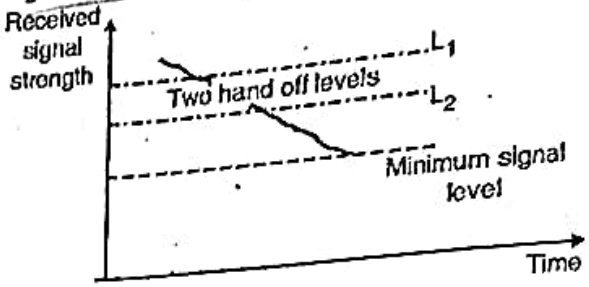
- The hand off is known as soft handoff if the MS starts communication with a new base station without stopping the communication with the older base station.
- In a soft hand off the operating frequencies of the old and new base stations are identical.
- Soft hand off enhances the signal by providing different-site selection diversity.
- In simple words we can say that the soft hand-off is based on the Make before Break strategy. This technique is used to lower the rates of call drops,
- Soft hand-off is used in CDMA systems.

3. Softer hand off :

- If the handoff takes place within the same cell then it is known as softer hand off.

4. Delayed hand off (Two level hand-off) :

- In many situations, instead of one level, a two level handoff procedure is followed, in order to ensure a higher possibility of a successful handoff.
- A hand off can be delayed if no available cell could accept the call. Fig. 2.4.3 shows a graph of signal strength with two handoff levels.



(G-1415) **Fig. 2.4.3 : A two level handoff scheme**

- When the signal level drops below the first handoff level, the MS initiates a hand off request.
- If due to some reason the mobile unit is in a hole (Place in a cell with low signal level) or neighbouring cell is busy then the MS will repeat the handoff request after every 5 seconds.
- But if the signal strength drops down further and reaches the second handoff level (L_2) then the handoff will take place without any condition, immediately.
- This process is called as **delayed hand off.**

Advantages :

1. It is possible to delay the handoff if neighbouring cells are busy.
2. The number of hand offs required to be carried out will reduce.
3. This will allow the processor to handle calls more efficiently.
4. It makes the handoff occur at the proper location and eliminates the possible interference in the system.

5. Forced handoff :

- A **forced handoff** is defined as the hand off which would normally occur but is not allowed to happen by force or a handoff that should not occur but is forced to take place.

6. **Queued handoff :**

- In the **queued handoff** process, the MTSO arranges the handoff requests in a queue instead of rejecting them, if it finds that new cell sites are too busy to makes the handoff possible.
- These handoff requests are then acted upon in a sequential manner. Queueing of handoffs is more effective than the two threshold handoff.
- Also, a queueing scheme is effective only when the handoff requests arrive at the MTSO in the form of batches or bundles.

7. **MAHO : Mobile Assisted Hand-Off :**

- In the second-generation (2G) systems, the hand off decisions is assisted by the mobile stations.
- The mobile assisted hand offs are known as MAHO.
- In MAHO, every mobile station measures the power it receives from all the base stations around it and continuously reports these measured power levels to the serving base station.
- If the power received from the base station of the neighbouring cell begins to go beyond the power received from the current base station by a certain margin then the hand off will be initiated.
- The advantage of MAHO is that this method reduces the time required to handover the call between the base stations.
- MAHO is particularly suitable for the microcellular environment where the hand off procedure needs to be followed very frequently.

8. **Inter cell handoff :**

- During an ongoing call, if a mobile station moves from one cell to another cell, then the corresponding handover is known as inter cell hand-off.
- Thus the inter cell hand-off switches a call in progress from one cell to the other cell.

9. **Intra cell hand-off :**

- The Intra cell handover is the handover within one sector or between different sectors of the same cell.
- It does not require network connections to be altered.
- The intra cell handover switches a call in progress from one channel to the other channel of the same cell.

2.5 Global System for Mobile (GSM) :

Definition :

- The Global System for Mobile Communications **(GSM)** is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets.
- Various mobile systems developed over the years are GSM, NA-TDMA, CDMA, PDC etc.
- The only multiple access technique in analog cellular systems is FDMA (frequency division multiple access) but the digital cellular systems can use either TDMA or CDMA for them.
- The long form of **GSM** is global system for mobile communications, it is a digital mobile system and it uses **TDMA** for multiple access.
- We know that in TDMA each user is allowed to use the radio channel only for a fixed duration of time.
- During this time slot, the user is allowed to utilize the entire bandwidth of the channel.
- Therefore the data is transmitted in the form of bursts.
- A European group called CEPT began to develop the GSM-TDMA system in 1982.
- The first GSM system was implemented in Germany in 1992. It was named as D_2.

- GSM is a second generation cellular system standard. It was developed in order to solve the fragmentation problems of the first generation cellular systems. GSM is the world's first cellular system to specify the digital modulations.

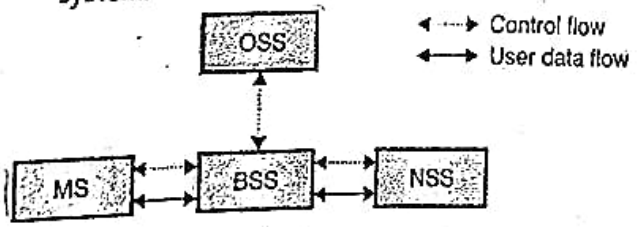
GSM : The European TDMA Digital Cellular Standard :

- Global System for Mobile is world's first cellular system based on digital modulation. By the mid-2010s, it achieved over 90 % market share, and started operating in over 193 countries.
- The 2G networks were developed as a replacement for first generation (1G) analog cellular networks.
- The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony.
- A GSM system has maximum 200 full duplex channels per cell.
- Each cell has different uplink and downlink frequency.
- It uses a combination of FDM, TDM and slotted ALOHA to handle the channel access.

2.6 GSM System Architecture :

Simplified block diagram :

- Fig. 2.6.1 shows the basic architecture of a GSM system.



(D-895) **Fig. 2.6.1 : GSM architecture**

- It shows that the GSM system consists of many subsystems such as :
  1. Mobile station (MS).
  2. Base station subsystem (BSS).
  3. The network and switching subsystem (NSS).
  4. Operating subsystem (OSS).

1. **Mobile station (MS) :**

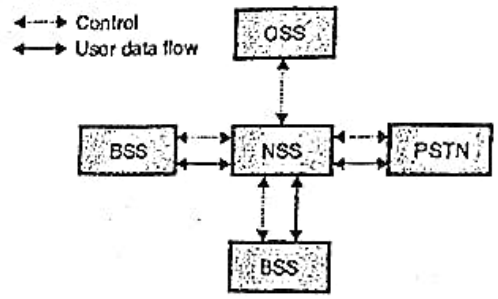
- This equipment is used to support the connections of the external terminals such as a PC or FAX.

2. **Base station subsystem (BSS) :**

- The BSS and MS are connected to each other via a radio interface.
- It is also connected to NSS in the same way. GSM operation is based on the open system inter connection (OSI) model.

3. **Network and switching subsystem (NSS) :**

- NSS as shown in Fig. 2.6.2 uses an intelligent network (IN).



(D-896) **Fig. 2.6.2 : NSS external environment**

- A signaling NSS is one of the main switching function of GSM.
- The primary job of NSS is the management of the communication between GSM users and other communication users.

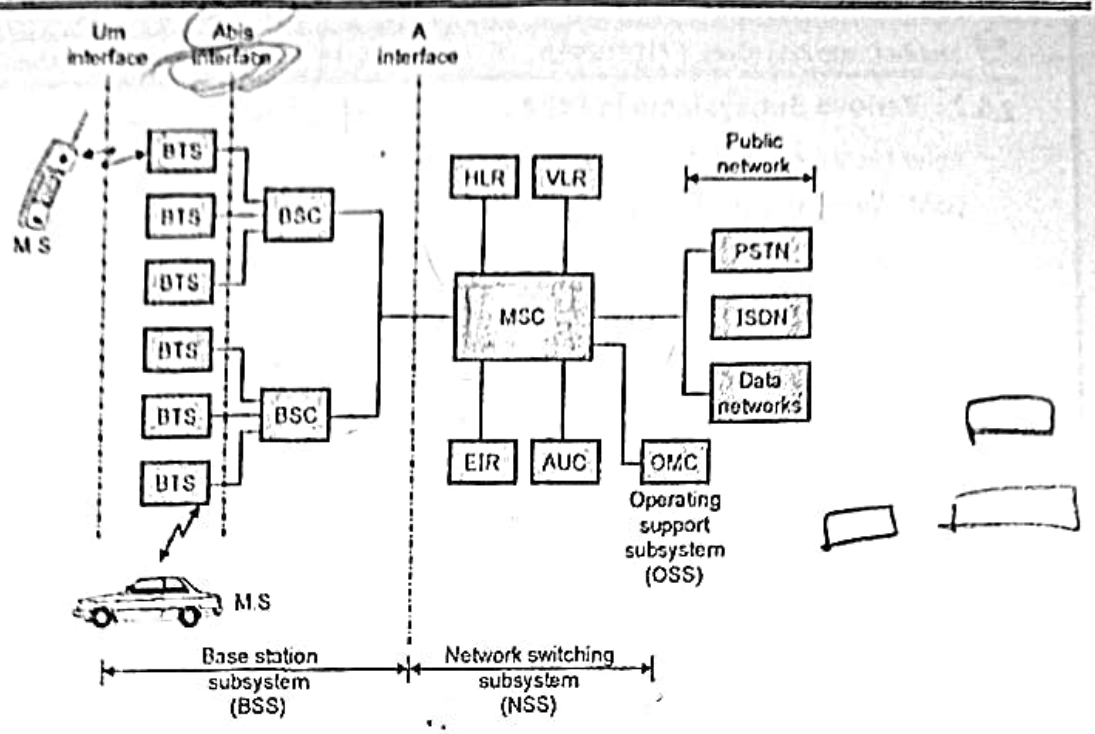
4. **Operating support subsystem (OSS) :**

- The OSS takes care of the following areas of operation :
  1. Network operation and maintenance.
  2. Charging and billing
  3. Management of mobile equipment.

2.6.1 Detail Architecture of GSM :

Block diagram :

- The detail architecture of a GSM system is shown in Fig. 2.6.3.
- The BTS and BSC both are part of the Base Station Subsystem (BSS).



BTS : Base Transceiver Station BSC : Base Station Controller

HLR : Home Location Register VLR : Visitor Location Register

MSC : Mobile Switching Centre EIR : Equipment Identity Register

AUC : Authentication Center OMC : Operation Maintenance Center

(GT-8) **Fig. 2.6.3 : GSM system architecture**

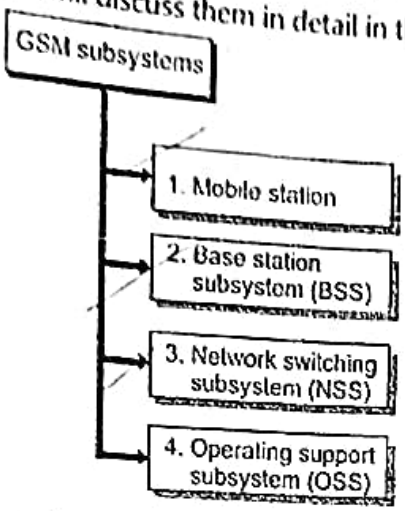
- Each BSC has hundreds of BTSs. (Bus Transceiver Stations) connected to it.
- These BTSs are controlled by the corresponding BSCs. The BTSs are connected to BSCs either physically or via microwave links or dedicated leased lines.
- The interface between BTS to BSC is called as **Abis interface.**
- This interface is expected to carry the voice data (traffic) and maintenance data.
- The BSCs are physically connected to MSC (Mobile Switching Center) via dedicated / leased lines or microwave link. This interface is known as the **A interface.**
- The NSS contains three different databases, called Home Location Register (HLR), Visitor Location Register (VLR) and Authentication Center (AUC).
- The **HLR** is a database containing the subscriber information and location information of each user, who is staying in the same city as MSC.
- Each subscriber is assigned a unique International Mobile Subscriber Identity (IMSI) and this number will identify each user.
- **VLR database** is used to temporarily store the IMSI and customer information for each roaming subscriber.
- **AUC** is the strongly protected database which takes care of authentication and handles the encryption keys for all the subscribers in HLR and VLR.
- The OSS supports one or more Operation Maintenance Centers (OMC).
- The OMC is used for monitoring and maintaining the performance of each MS, BS, BSC and MSC used in a GSM system.

Modulation :

- The GSM uses the Gaussian minimum shift keying (GMSK) as its modulation technique.

2.6.2 Various Subsystems in GSM :

- Refer Fig. 2.6.4 which shows various subsystems in GSM. We will discuss them in detail in this section.



(GT-10) **Fig. 2.6.4 : Different subsystems in GSM**

2.6.2.1 MS (Mobile Station) :

Definition :

- MS is defined as the physical mobile handset or equipment used by the subscriber to access the GSM network.
- A mobile station may include :
  1. MT : Mobile Termination
  2. TE : Terminal Equipment
  3. TA : Terminal Adapter.

Types of MS :

- Types of MS are as follows :
  1. Vehicle mounted station
  2. Portable station
  3. Handheld station.
- In practice MS is divided in two parts : a mobile terminal (MT) and a SIM.
- **A mobile terminal** consists of hardware and software.
- It is simply the mobile handset, which manages all the functions related to radio and human interface.
- **SIM (Subscriber Identity Module)** is a small card, plugged into mobile terminal.
- The mobile service providers provides a SIM card for every GSM subscriber.
- It is microprocessor based entity implemented on smart card.
- MS cannot communicate with any user or network unless it has the SIM card inserted in it.
- MS has various number identities as follows :
  1. IMSI - International Mobile Subscriber Identity
  2. TMSI - Temporary Mobile Subscriber Identity
  3. IMEI - International Mobile Equipment Identity

2.6.2.2 BSS (Base Station Subsystem) :

Definition :

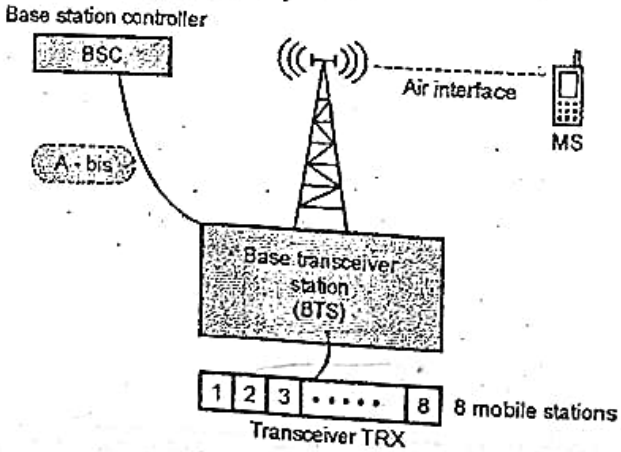
- The BSS or base station subsystem is a GSM subsystem, which manages all the signalling and traffic between MS and NSS.
- BSS is connected to MS and NSS via a radio interface.

Functions of BSS :

- Functions performed by BSS are as follows :
  1. Coding of speech channels,
  2. To allocate the available radio channels to mobile stations on request,
  3. To transmit the paging signals,
  4. To transmit and receive both control and data signals over the air interface.

Block diagram :

- Fig. 2.6.5 shows the simplified block diagram of the base station subsystem.



(G-2734) **Fig. 2.6.5 : Base station subsystem (BSS)**

- The BSS consists of a BTS (Base Transceiver Station) and a BSC (Base Station Controller).

1. BTS (Base Transceiver Station) :

- As shown in Fig. 2.6.5 a BTS consists of a directional antenna equipment to transmit and receive radio signals.
- The transceiver (TRX) acts as the central unit of the BTS.
- The TRX manages wireless links between up to 8 MSs by using a single pair of frequencies.
- The TRX also an important device called TRAU (Transcoder Rate Adaptation Unit) for encoding and decoding of the speech and rate adaptation function of the data.
- A BSC is connected to and controls multiple BTSs, out of which some are co-located at the BSC and others may be remotely distributed and connected to the BSC through microwave links or dedicated lease lines.

2. BSC (Base Station Controller) :

- A BSC is a high quality switch, which controls hundreds of BTSs simultaneously.
- A BSC controlling two BTSs, itself handles the mobile handovers between them without involving the MSC. This reduces burden on the MSC.
- The other function of BSC is to provide cell configuration data and to control of RF power levels in BTSs.
- It also assigns free radio channels in the TRX for the link to the mobile station.
- BSC is also maintains the radio path between MSs during the call and disconnects it when the call is over.

2.6.2.3 NSS (Network Switching Subsystem) :

- As shown in Fig. 2.6.5 the Base Station Subsystem (BSS) forwards the signals to the Network Switching Subsystem (NSS), which consists of main switching center (MSC), various databases and mobility management units.
- The main unit of NSS is MSC (Mobile Switching Center).
- There are the following five functional entities associated with the MSC :
  1. HLR : Home Location Register
  2. VLR : Visitor Location Register
  3. EIR : Equipment Identity Register
  4. AUC : Authentication Center
  5. GMSC : Gateway MSC
- The function of NSS is to manage the communication between GSM network and users from other networks like PSTN, ISDN, Data networks etc.

Mobile Switching Centre (MSC) :

- MSC (Mobile Switching Center) is the main unit of NSS.
- Functions performed by MSC are as follows :
  1. To perform all the necessary switching functions required by MSs located in MSC area.
  2. To communicate with other MSCs present in the GSM network.
  3. To communicate with the other networks like PSTN etc.
  4. To track the location of the subscriber to carry out the handover process whenever necessary.
  5. To perform all the necessary interworking functions.
  6. To perform the call routing and echo control functions.

1. HLR (Home Location Register) :

- HLR is the database of permanent subscriber information, which contains important user information like address, account status and preferences.
- The HLR stores the following two types of information :
  1. Subscriber information
  2. Mobile information

- **HLR** performs the following **functions.**
  1. **Identification** : HLR stores two very important numbers called IMSI and MSISDN. (Mobile Station International Subscriber Directory Number), which are used in call routing between MSC and a particular MS. These unique numbers are necessary to identify a particular MS.
  2. **Subscriber service provision :** HLR also provides information about the offered services such as, teleservices, bearer services or supplementary services.
  3. **VLR address :** The VLR address is required (which is a temporary data), when MS is roaming. It also provides the cipher keys for encryption and decryption.

2. **VLR (Visitor Location Register) :**

- VLR database is used to temporarily store the IMSI and customer information for each roaming subscriber.
- Whenever a roaming MS enters the new MSC area it undergoes registration process as follows:

Registration process :

1. VLR identifies that the particular MS belongs to some other MSC area.
2. VLR communicates with HLR in the home network of that MS.
3. VLR constructs the GT (Global Title) from IMSI so as to allow communication between VLR and Home HLR.
4. VLR generates MSRN (Mobile Subscriber Roaming Number) to allow MS to use the current network when in roaming.
5. MSRN is sent to home HLR as well.

- VLR stores the following :
  1. MSRN
  2. TMSI
  3. Home location of the MS
  4. Supplementary services data of MS
  5. MSISDN
  6. IMSI
  7. GT
  8. Local MS identity if used VLR works in association with HLR and AUC.

3. **EIR (Equipment Identity Register) :**

- It is the database of all the legitimate, and faulty MSs. It stores IMEI of every MS, which is provided by the equipment manufacturer.
- Its function is to keep track of all the valid and invalid mobile equipment in the area.

4. **AUC :**

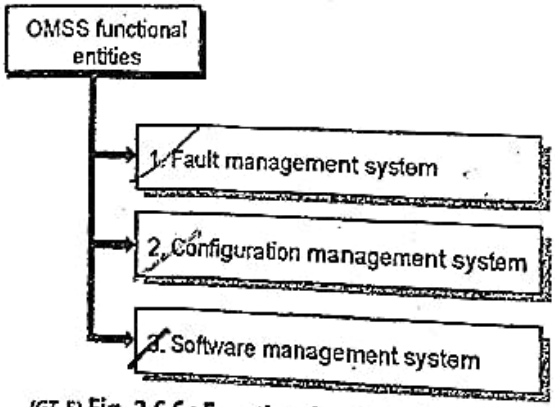
- AUC is the database that stores the secret authentication keys for each subscriber.
- It also generates security related parameters for protection purposes. The same secret key is stored in SIM card.
- The secret key is never transmitted on air for security reasons. AUC always works with HLR to carry out authentication successfully.

5. **GMSC :**

- All the calls to a GSM network are routed through GMSC which first identifies the correct HLR and authenticates it.
- It also communicates with other networks and provides gateway function for external network communication with GSM network.

2.6.3 OMSS : Operation and Maintenance Subsystem :

- The three functional entities in OMSS are as shown in Fig. 2.6.6.



(GT-5) **Fig. 2.6.6 : Functional entities in OMSS**

- The fault management system invokes alarms from the BSS elements when there is a fault.
- The fault is then resolved either by software or by technicians.

- The function of the Configuration Management is to install and maintain the software of the newly setup BSS network elements.
- It's other functions include management of hardware inventory list and changing operation parameters like frequencies of BTS etc.
- The software management system installs new software or updates and manages the software inventory lists.

2.6.4 Characteristics / Features of GSM Standard :

- Some of the important characteristics/features of GSM standard are as follows :

1. GSM can support more subscribers in the given spectrum.
2. The short messaging service (SMS) is provided by the GSM standard, that allows its subscribers to transmit and receive character text messages.
3. GSM has a subscriber identity module (SIM), which is a memory device that stores all the important information like subscriber's identification number.
4. Each subscriber is allotted a four digit personal ID number that activates service from any GSM phone. The SIMs are smart cards or plug-in modules. Each subscriber needs to insert his SIMs into a mobile phone, to receive GSM calls to the number irrespective of the location.
5. The GSM system provides the **on-the-air privacy** by encrypting the digital bit stream sent by the GSM transmitter.
6. The same GSM phone can be used in different networks.
7. The data transmission and reception rate supported across GSM networks is 9600 bps.
8. GSM also supports FAX transmission and reception at 9.6 kbps.
9. The size of GSM handsets is much smaller.
10. GSM supports the facilities like call forwarding, call on hold, conferencing, Calling Number Identification Presentation (CLIP) and international roaming.
11. GSM is compatible with ISDN , PSTN as well as other telephone company services.

- Following are the two most important GSM features :
  1. Subscriber Identity Module (SIM).
  2. On air privacy.

1. Subscriber Identity Module (SIM) :

- The SIM card of a GSM phone is nothing but a memory device that stores some very important information like, identification number of the subscriber, the type of network and the countries in which the services can be provided to the subscriber.
- In addition it also stores the unique privacy key for the subscriber for decrypting the encrypted received messages and other important information.
- A SIM is required to activate service for any GSM phone.
- Without a SIM all GSM mobile phone cannot operate.

2. On air privacy :

- On-air privacy is the second important feature of GSM.
- On-air privacy indicates that the GSM system ensures some kind of privacy of the transmitted signal.
- The analog FM cellular system calls can be easily monitored because no on air privacy is provided.
- However the GSM transmitters use encryption to encode the signals before transmitting them which makes them a lot safer and hard to monitor.

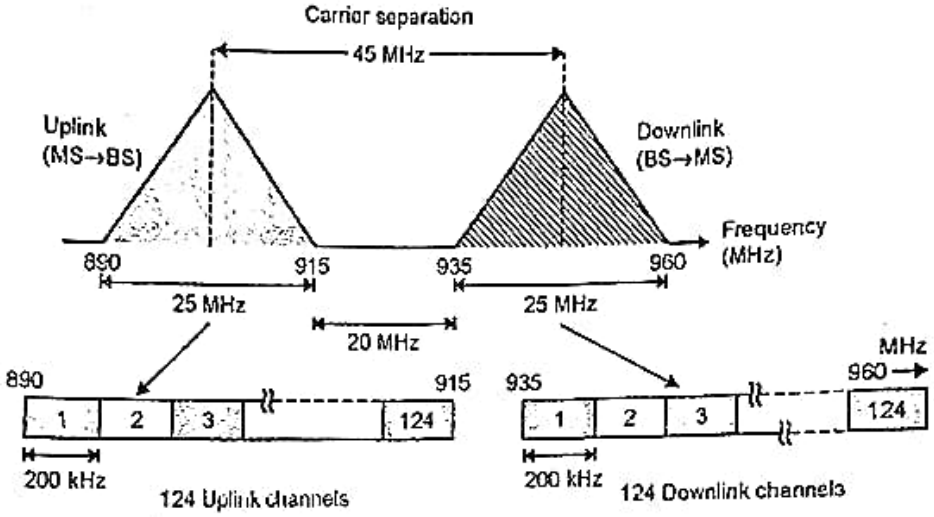
2.7 Frequency Allocation in GSM :

- Radio transmission parameters are the important parameters of the GSM standard, related to the transmission of data or signals.

- They include the frequencies used for forward and reverse transmission, bandwidths, duplexing technique, number of time slots, number of users, etc.

Frequency bands :

- The frequency bands in GSM have been shown in Fig. 2.7.1(a).
- Two bands, one for the **uplink** and the other for **downlink**, each with a bandwidth of 25 MHz, have been assigned to the GSM system.
- The frequency band assigned for the **uplink** is from 890 MHz to 915 MHz (uplink is transmission by mobile stations to base stations).
- Fig. 2.7.1(a) shows the spectrum of GSM standard.

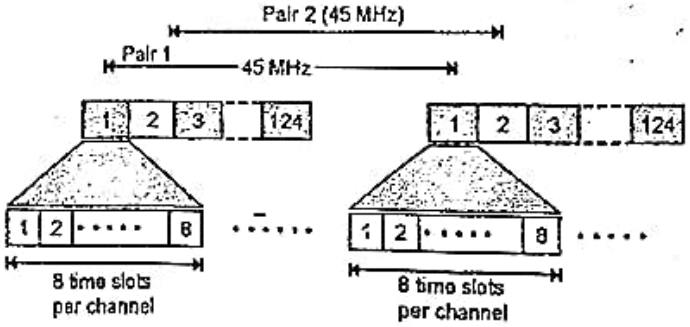


(GT-3) **Fig. 2.7.1(a) : GSM frequency bands**

- The frequency band assigned for the **downlink** is from 935 MHz to 960 MHz (downlink is transmission by base stations to mobile stations).
- These frequency bands are assigned to GSM in Europe and this GSM is known as GSM 900.
- A duplex transmission is realized in a Frequency Division Duplex **(FDD)** mode.
- That means two different sets of frequencies are used for the uplink and downlink.
- Each of the 25 MHz band is divided into 124 frequency bands or channels of 200 kHz each with carrier frequencies in their centers (Note that 124 × 200 kHz = 24.8 MHz).
- These frequency channels are assigned to various cells in a sector.
- The ARFCN denotes a forward and reverse channel pair which is separated in frequency by 45 MHz and each channel is time shared between as many as eight subscribers using TDMA.
- Each of these eight subscribers uses the same ARFCN and occupies a unique timeslot (TS) per frame.

2.7.1 Type of Multiple Access :

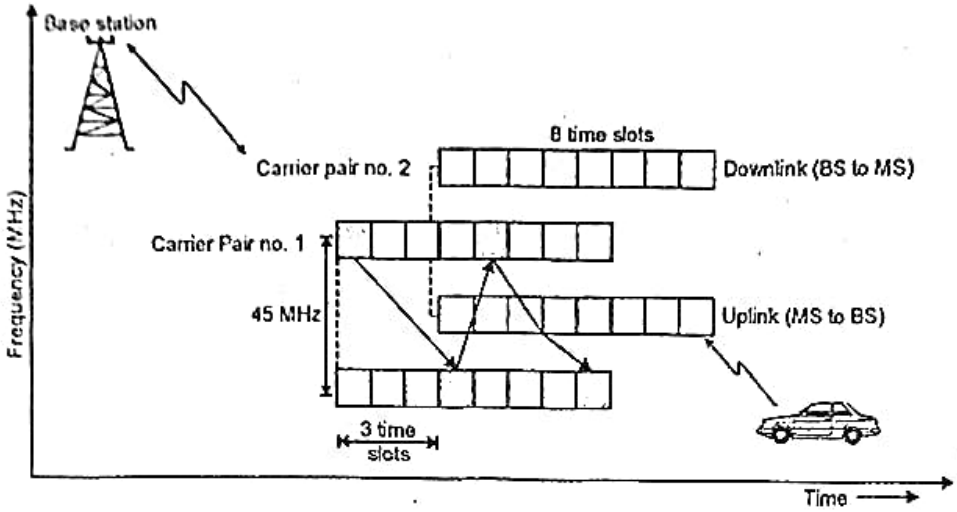
- Time along each carrier is divided into 8 slots as shown in Fig. 2.7.1(b).



(G-2735) **Fig. 2.7.1(b) : Uplink / Downlink channels and time slots in GSM**

- Thus, multiple access is realized by assigning the connection a particular carrier frequency (or a sequence of them if frequency hopping is performed) and a selected time slot.
- Therefore we may treat the GSM as a system with TDMA/FDMA multiple access scheme.
- Physical channels are arranged in pairs. Each pair consists of one physical channel in each direction (uplink and downlink).

- They are marked with the same time slot number and the carrier separation is equal to 45 MHz as shown in Fig. 2.7.1(b).
- Due to frequency planning, a subset of carrier frequencies is assigned to each cell or its sector as per some specific rules.
- Fig. 2.7.2 depicts the frequencies and time slot assignment in the GSM system.



(G-2738) **Fig. 2.7.2 : Frequency and time structure of GSM channels**

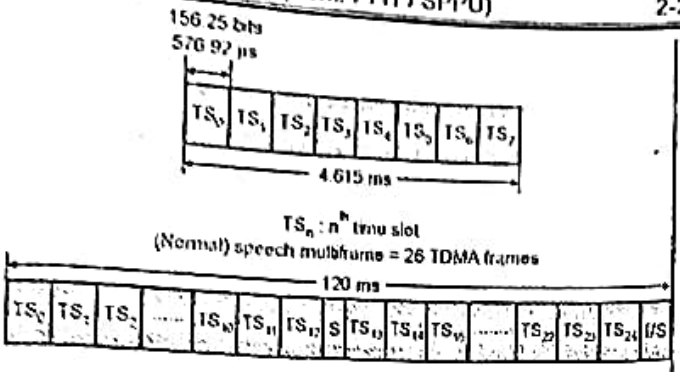
- It shows that the numbering of the time slots is delayed by three in downlink as compared with uplink transmission.
- This has been done to ensure that, a mobile station connecting to a base station in the assigned time slot never transmits and receives the signals at the same time.
- In this manner, an electromagnetic feedback between a mobile station transmitter and receiver is avoided.
- The transmitter and the receiver can share the computational power between them.
- None of the carriers and time slots are devoted to a particular exclusive use.
- It means that the carriers and time slots can be used to perform different functions depending on the carrier and the current state of the system.
- For that reason the GSM standard has introduced the concept of a **logical channel**, which is a structure performing a particular task in the system.

Channel data rate :

- Radio transmissions on both the forward and reverse link are made at a channel data rate of 270.833 kbps (1625.0/6.0 kbps) using binary BT = 0.3 GMSK modulation.

Channel transmission rate per user :

- Thus, the signaling bit duration is 3.692 μs, and the effective channel transmission rate per user is 33.854 kbps (270.833 kbps/8 users).
- With GSM overhead, user data is actually sent at a maximum rate of 24.7 kbps.
- Each TS (time slot) has an equivalent time allocation of 156.25 channel bits, but of this, 8.25 bits of guard time and six total start and stop bits are provided to prevent overlap with adjacent time slots.
- Each TS has a time duration of 576.92 ms as shown in Fig. 2.7.3, and a single GSM TDMA frame spans 4.615 ms.



Tn : nth TCH frame
S : Slow associated control channel frame
I : Idle frame

(G-2780) **Fig. 2.7.3 : The speech dedicated control channel frame and multiframe structure**

- The total number of available channels within a 25 MHz bandwidth is 125 if we assume that there are no guard bands.
- Since each radio channel consists of eight time slots, there are thus a total of 1000 traffic channels within GSM.
- In practical implementations, a **guard band** of 100 kHz is provided at the upper and lower end of the GSM spectrum, and only 124 channels are implemented.
- Table 2.7.1 summarizes the GSM air interface.

A Physical Channel :

- The combination of a TS number and an ARFCN constitutes a physical channel for both the forward and reverse link.
- Each physical channel in a GSM system can be mapped into different logical channels at different times.
- That is, each specific time slot or frame may be dedicated to either handling traffic data (user data such as speech, facsimile, or teletext data), signaling data (required by the internal workings of the GSM system), or control channel data (from the MSC, base station, or mobile user).
- GSM provides explicit assignments of time slots and frames for specific logical channels, as described below.

2.7.2 GSM Specifications / GSM Air Interface :

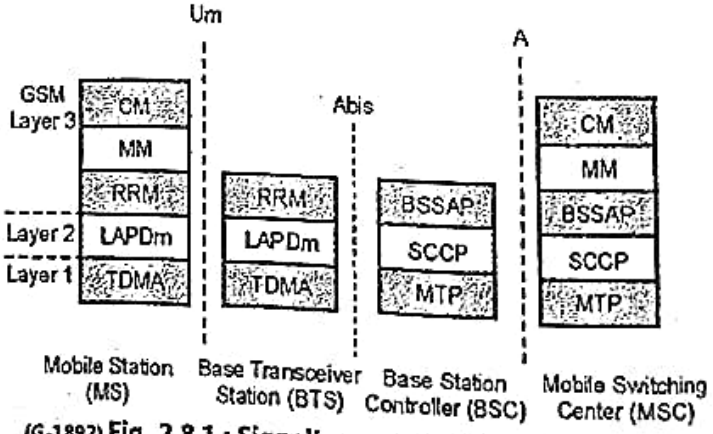
- Table 2.7.1 summarizes the GSM air interface specifications.

Table 2.7.1 : GSM air interface specifications

Sr. No.	Specification / Parameter	Value
1.	Uplink frequencies	890-915 MHz (Europe) 1850-1910 MHz (US PCS)
2.	Downlink frequencies	935-960 MHz (Europe) 1930-1990 MHz (US PCS)
3.	Frequency spectrum bandwidth	25 MHz
4.	Duplexing	FDD
5.	Multiple access	FDMA/TDMA
6.	Number of full duplex channel	124
7.	BW of each channel (carrier separation)	200 kHz
8.	Number of voice channels per carrier	8
9.	Type of modulation	GMSK
10.	Channel data rate	270.833 kb/s
11.	Frame duration	4.615 mS
12.	Time slot period	576.9 µS
13.	SIM card	Yes
14.	Handover type	Hard
15.	Modulation	GMSK

2.8 GSM Signalling Protocol Architecture :

- Fig. 2.8.1 shows the signalling Protocol Structure in GSM.



(G-1892) **Fig. 2.8.1 : Signaling protocol structure in GSM**

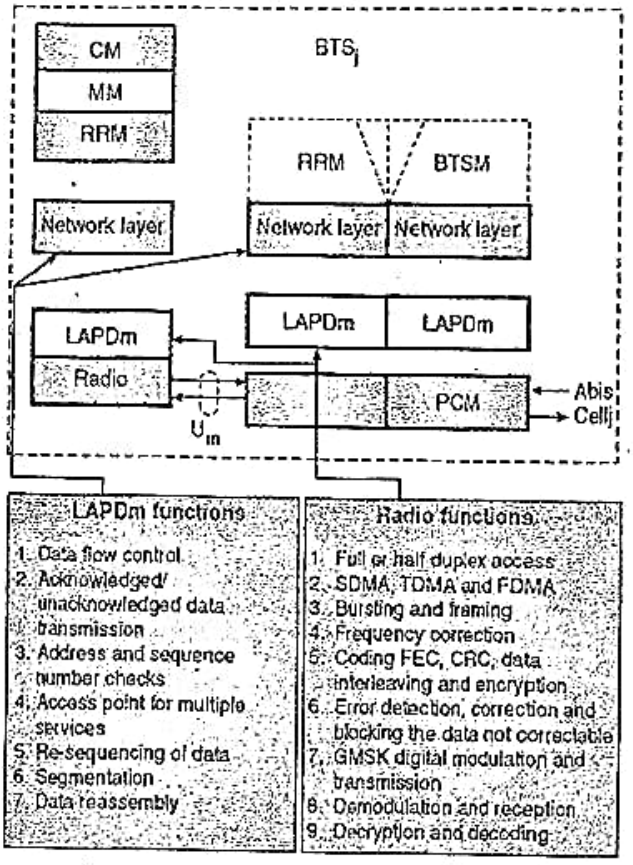
- In the signalling protocol structure in GSM there are three general layers depending on the interface.
- **Layer 1** is the physical layer. It makes use of the channel structures over the interface.
- **Layer 2** is data link layer. Across the U_m interface (Refer Fig. 2.8.1), the DLL is actually a modified version of the **Link Access Protocol D(LAPD)** used in ISDN. It is called as the LAPDm.
- Across the **A** interface, as shown in Fig. 2.8.1 the message transfer part layer 2 of signal system number 7 (SS7) has been used. The air interface of GSM consists of TDMA time slots and FDMA frequency bands.
- LAPDm protocol is used over the air interface between the base station trans-receiver and the mobile device.
- Some additional control information, apart from the actual data is required to be used for transmitting the information to a desired destination.
- It is called as the signalling message.
- The signalling channels are time division multiplexed on an aggregate of the TDM slots.
- Layer-3 of the GSM signalling protocol is divided into the three following sub-layers :
  1. Mobility Management (MM).
  2. Radio Resource Management (RRM) and
  3. Connection Management (CM) for calls routing.
- The layer-3 protocol is used for different purposes of mobility, communication of network resources, code format and call related management messages between different network entities.
- The radio recourse management (RRM) between the Mobile Station and the Base Station Subsystem (BSS), can be implemented.
- Mobility Management and Connection Management is the communication between the Mobile Station and MSC (Mobile Switching Centre).
- The A interface uses an SS7 protocol called Signal Correction Control Protocol (SCCP) that supports communication between the MSC and BSS and the network messages between the individual subscribers and the MSC.

2.8.1 GSM Interfaces :

- As shown in Fig. 2.8.1 there are three different interfaces present in GSM system they are :
  1. U_m : Interface between MS and BTS.
  2. Abis : Interface between BTS and BSC.
  3. A : Interface between BSC to MSC.

2.8.2 Mobile Station-Base Transceiver Station Signaling Protocols :

- Fig. 2.8.2 shows the functions and protocol layers between the MS and BTS.



(G-1893) **Fig. 2.8.2 : Functions and protocol layers between the MS and BTS**

Radio interface / Physical layer :

- Radio (U_m interface) is the physical layer between the Mobile Station (MS) and the Base Transceiver Station (BTS).
- The data link layer is supposed to control the flow of packets sent to and coming from the network layer and provide access to different services.

- LAPDm (Link Access Protocol D-channel modified) is the data link layer protocol, which is located between MS and BTS.
- Refer Fig. 2.8.2 that enlists the functions of LAPDm.
- It does not use any flag for frame delimitation. Instead, the frame delimitation is taken care of by the physical layer that defines the frame boundaries.
- The information carrying field in LAPDm is differentiated field from the fill-in bits (used to fill the transmission frame) with the help of the length indicator.
- A 3-bit Service Access Point Identifier **(SAPI)** used as an address field in LAPDm. It can take eight different values from 0 to 7.
- Out of them, SAPI 0 is used for call control, MM and RRM signaling where as SAPI 3 is used for SMS.
- All other fields are reserved for future purpose.

Network layer sub layers :

- The network layer has the following three sub layers:
  1. Connection Management (CM)
  2. Mobility Management (MM)
  3. Radio Resource Management (RRM)

1. Connection Management (CM) for calls routing :

- The CM sub layer protocol has been designed to support the following three aspects of a call :
  1. Call establishment,
  2. Call maintenance and
  3. Call termination.
- It also controls and supports the functioning of SMS, supplementary services and DTMF signaling.

2. Mobility Management (MM) :

- This network sub layer has been designed to handle the issues related to mobility management when a mobile station travels from one cell to the other.
- The functions of MM are as follows :
  1. Registration.
  2. Update the location.
  3. Authentication
  4. Identification.
  5. Maintaining a reliable communication with the upper layers.
  6. To use TMSI allocated by VLR in place of IMSI at HLR.

3. Radio Resource Management (RRM) :

- This network sub layer is supposed to handle the following issues in setting up point-to-point communication between a mobile device and network : establishment, maintenance and release of RRM connection.
- RRM is used for data and user signaling.
- This sub layer carries out procedures such as, selection, reselection, and the hand off process.
- When RRM is established, it handles the reception of BCCH and CCCH as well.
- A mobile station always initiates the RRM session, either in response to a paging message or in order to make a call.
- The functions of RRM are as follows :
  1. To manage the quality of radio link.
  2. Assignment of frequency.
  3. It provides options for frequency hopping sequence.
  4. Measurements of signal strength.
  5. To manage the handover process.
  6. RRM session management.
  7. To manage synchronization.

2.8.3 Abis Interface / Base Transceiver Station (BTS)-Base Station Controller (BSC) Signaling Protocols :

- The interface between the BTS and BSC that carries out the traffic and maintenance data is the known as the **Abis interface** which is standardized for GSM systems.

- A wired network such as PSTN, ISDN, PSPDN etc. is used to connect the BTS and BSC.
- The voice signal is encoded into the 64 kbps PCM format in a PSTN network.
- The same format is also used by the Abis interface.
- PCM coding techniques are different from 22.8 kbps. TCH radio interface U_m (between MS and BTS). Therefore a translation between the coding formats is essential.
- This is done by translating the TCH bits received from caller mobile station (MS) to 64 kbps PCM and then from PCM to TCH for receiver MS.
- The voice quality gets affected due to the translation and retranslation.
- Therefore, a procedure called **TFO (tandem free operation)** is adopted, to improve the voice quality at the BTSs, BSCs and MSCs.
- The data link layer protocol for the Abis interface between the BTS and BSC is **LAPD (link access protocol D channel)** which prescribes the standard procedure for D-channel of ISDN.
- The network layer protocol between the BTS and BSC is called as BTSM (BTS management).

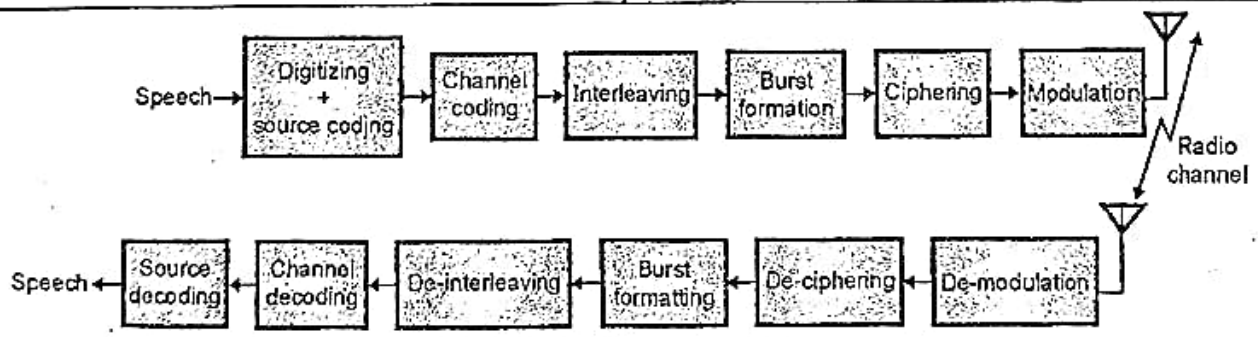
2.8.4 A Interface / Base Station Controller (BSC) – Mobile Switching Centre (MSC) Signaling Protocols :

- The physical layer between the BSC and MSC uses PCM multiplexing.
- The MSC is connected to the networks such as PSTN, ISDN and other data networks that use either 64 kbps PCM or 2.048 Mbps CCITT that carries 32 PCM channels.
- The interface between BSC and MSC is the A interface.
- The type of communication between BSCs and MSCs is wired communication.
- MTP (message transfer protocol) and SCCP (signal correction control protocol) are the two data link layer protocols between the BSC and MSC.
- Both of them are parts of SS7 (Signaling System No. 7) used by A interface.
- The network layer protocol that is used at BSC is BSSAP (Base Sub System Application Protocol).

Signal Processing in GSM :

Block diagram :

- Refer Fig. 2.9.1 which shows the block diagram, to understand all GSM operations from transmitter to receiver.



(G-1216) **Fig. 2.9.1 : GSM signal processing**

1. Speech coding :

- The working of speech coding in GSM is based on the principle of Residually Excided Linear Predictive Coder (RELP) which uses a Long Term Predictor (LTP).
- The operation of GSM speech coder makes use of a very interesting fact that, each person speaks for about 40 % of the total conversation time in a normal conversation.
- Therefore GSM works in the discontinuous transmission mode (DTX) by using a voice activity detector (VAD).
- Due to DTX mode the battery life increases and reduces the radio interference.

1. If the called mobile phone is switched off, a message can be played or recorded in the users voice mail.
2. If the mobile user has his subscription charges and bill pending, a message can be played and the call may not routed.

Step 4 : If all the conditions for routing the call are satisfied, then the MSC sends a request to VLR to determine the VLR the location of called mobile phone.

Step 5 : If the VLR is the home network, then it will find the Location Area (LA) of the mobile subscriber and will page and determine the location of the phone within the Location Area.

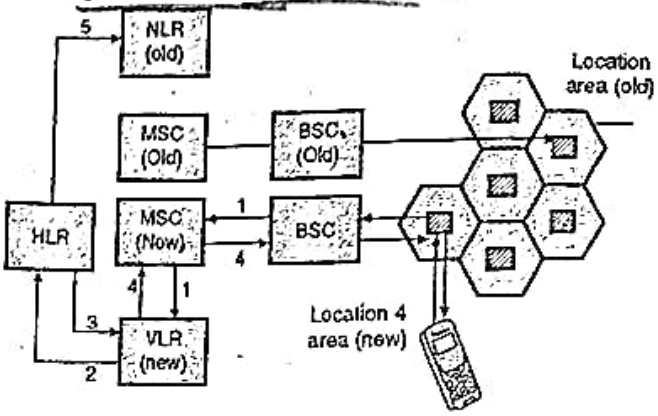
Step 6 : If the VLR has a different PLMN (Public Land Mobile Network), then it will route the call to foreign PLMN through the GMSC (gateway MSC) to the mobile subscriber.

2.10 Call Establishment in GSM :

- In this section we will discuss the following call flow sequences related to GSM :
  1. Registration / Location updating.
  2. Mobile terminated call
  3. Mobile originated call

1. Location updating :

- In order to receive the incoming calls from a mobile station that moves within and outside the service area, the home network should somehow keep a track of the location of all the active mobile stations.
- The location updating feature is activated when a mobile station either moves to other MSC or tries to access the network and is not registered in the VLR of that location.
- Each service area consists of many adjacent cells recognized by location area identities (LAI).
- The mobile station (MS) generally has the information from the neighbouring base stations and if it sees that a subscriber has moved to a new location then it initiates the sequence as shown in Fig. 2.10.1 and following steps.



(G-1773) **Fig. 2.10.1 : Location updating in GSM**

Location Updating Procedure :

Step 1 : When a new location is identified, the mobile station (MS) sends a request for location update to the new VLR via the BSC and MSC.

Step 2 : The location update message is sent to the HLR from the VLR. This message consists of the address of the VLR (new) and the IMSI of the MS.

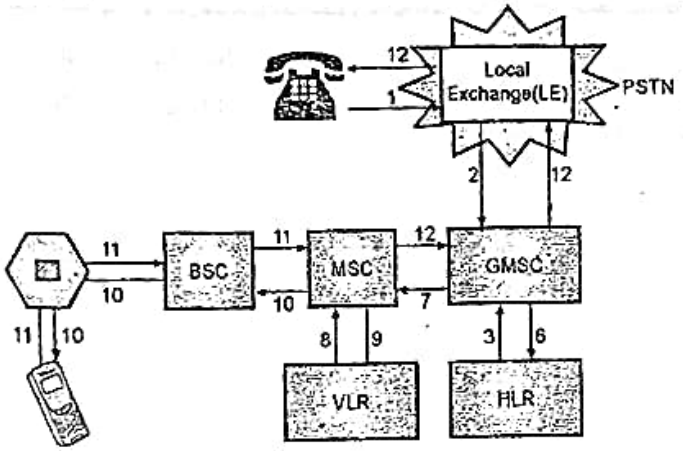
Step 3 : The security and service related information for the MS is transferred to the new VLR.

Step 4 : An acknowledgement message is sent to the mobile station as soon as the location update is done successfully.

Step 5 : The HLR instructs the old VLR to delete all the information related to the relocated MS.

2. Mobile terminated call :

- A call originating from PSTN and terminating on a mobile station is called as the mobile terminated call. Fig. 2.10.2 shows the steps in which a mobile terminated call is processed by GSM.



(G-1774) **Fig. 2.10.2 : Mobile terminated call in GSM**

Step 1 : The call originating landline user dials the Mobile Station ISDN of the mobile user (called party) in GSM.

Step 2 : The Local Exchange sends the call to the GMSC of the called GSM subscriber.

Step 3 : The GMSC searches the HLR for the GSM to obtain the desired routing number.

Step 4 : The HLR requests the current VLR of the called MS to obtain a Mobile station Roaming Number so as to rout the call to the correct MSC.

Step 5 : The current VLR sends the mobile station roaming number to the HLR.

Step 6 : The HLR sends the mobile station roaming number to the GMSC.

Step 7 : The GMSC transfers the call to the MSC by using the MS roaming number.

Step 8 : The MSC enquires about the Location Area Identity (LAI) of the mobile station subscriber to the VLR.

Step 9 : The VLR passes the LAI of the mobile station subscriber to the MSC.

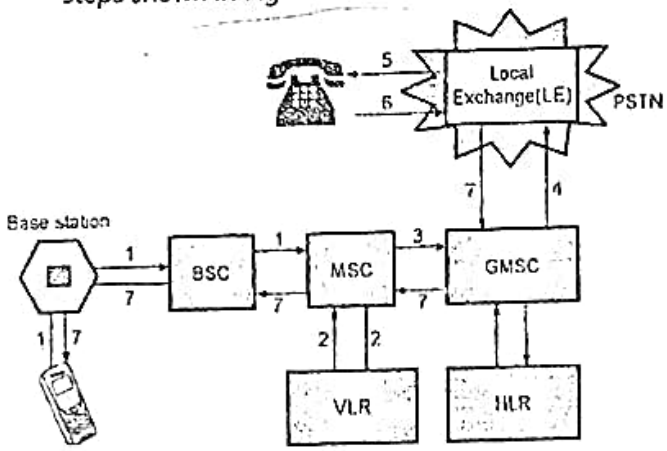
Step 10 : The MSC sends a pager message to the Mobile Station subscriber through BSC. The Mobile Station then sets up the required signaling links.

Step 11 : After establishing the signaling links, the BSC informs the MSC about the same and the call is delivered to the mobile station subscriber.

Step 12 : The connection to the calling landline is completed after the mobile subscriber answers the call.

3. Mobile Originated Call :

- This type of call is originated by a mobile subscriber and it is meant for a landline user.
- First the calling mobile subscriber enters the phone number to be called on the mobile and presses the send key.
- Then the mobile station connects the correct signaling links to the BSC.
- After that the call is processed by following the steps shown in Fig. 2.10.3.



(G-1775) **Fig. 2.10.3 : Originating mobile call in GSM**

Step 1 : The mobile station passes on the dialled number to the MSC via BSC to indicate that it needs service.

Step 2 : The VLR tells the MSC if the mobile station can access the requested service or not. If the MS can access the requested service, then the MSC instructs the BSC to assign the resources required for the call.

Step 3 : The allowed call is then routed to GMSC via MSC.

Step 4 : The GMSC then routes the call to the Local Exchange (LE) of called landline subscriber.

Step 5 : The LE then gives a ring on the called landline terminal.

Step 6 : The landline terminal returns an answer back tone to the LE.

Step 7 : The answer back tone is sent back to the Mobile Station thus completing the call.

2.11 Handover in GSM :

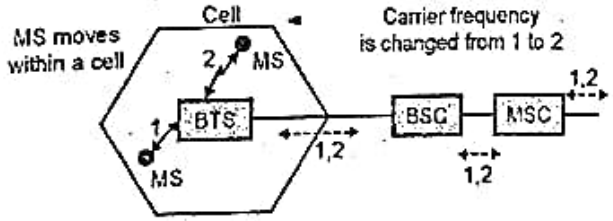
- We have already discussed the concept and need of handover in cellular systems.
- With reduction in the size of a cell, the number of handovers increases. However a handover is not supposed to cause a cut-off (also called as a call drop).
- The maximum duration for a handover in GSM has been decided to be equal to 60 ms.

2.11.1 Types of Handover in GSM :

- There are four types of possible handovers in a GSM system.
- They are :
  1. Intra-cell handover.
  2. Inter cell, Intra BSC handover.
  3. Inter-BSC, Intra-MSC handover.
  4. Inter MSC handover.

1. Intra-cell handover :

- The intracell handover happens when a mobile station (MS) moves from one place to the other within a cell as shown in Fig. 2.11.1(a).

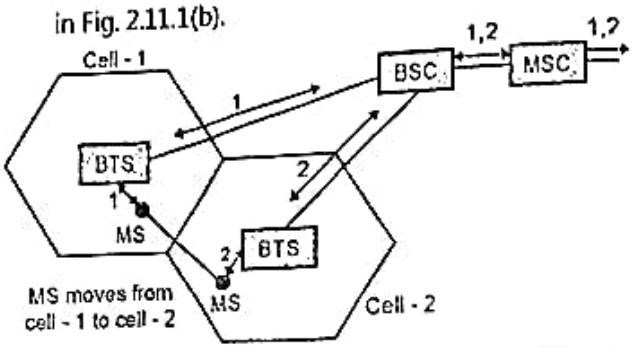


(GT-33) **Fig. 2.11.1(a) : The intracell handover in GSM**

- If a narrow band interference makes transmission at a certain frequency impossible, then the BSC can decide to change the carrier frequency.
- This will lead to the intra-cell handover.
- As shown in Fig. 2.11.1(a), the MS is operating on channel 1 when it is in its original position.
- When it moves within the cell to a new position, it is impossible to operate at this frequency due to interferences.
- Therefore the BSC changes its carrier frequency to 2 to reduce the interference.
- Thus the intracell handover procedure is performed either to optimize the traffic load in the cell or to improve the quality of a connection by changing the carrier frequency.

2. Inter-cell, Intra BSC handover :

- The intercell intra BSC handover has been shown in Fig. 2.11.1(b).

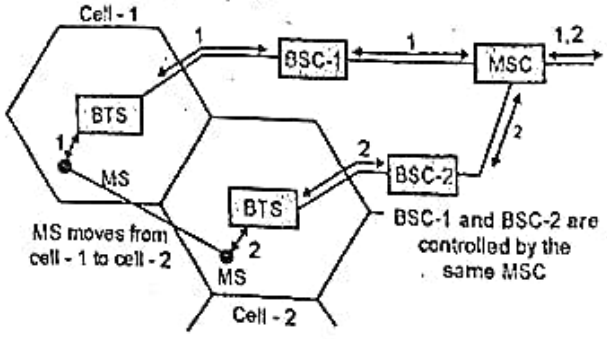


(GT-34) **Fig. 2.11.1(b) : Intercell intra-BSC handover in GSM**

- This type of handover takes place when a mobile station (MS), moves from one cell to the other (cell-1 to cell-2) but remains under control of the same BSC.
- The BSC will carry out the handover by assigning a new radio channel in the new cell to the MS and then release the old one.
- In Fig. 2.11.1(b) the MS is operating on channel-1 when it is in cell-1. As it moves to cell-2, the BSC will assign a new channel i.e. channel-2 to it when it enters into cell-2.

3. Inter BSC, Intra-MSC handover :

- The inter BSC intra MSC handover has been shown in Fig. 2.11.1(c).



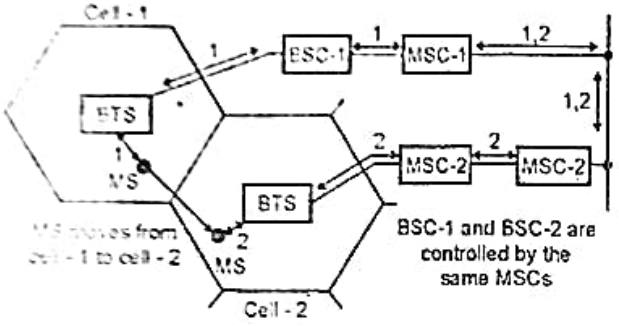
(GT-35) **Fig. 2.11.1(c) : Inter-BSC Intra-MSC handover in GSM**

- This type of handover takes place when a mobile station (MS), moves from one cell to the other (cell-1 to cell-2) controlled by different BSCs but same MSC.

- Such a handover is controlled by the MSC. The MSC will carry out the handover by assigning a new radio channel in the new cell to the MS and then release the old one.
- In Fig. 2.11.1(c) the MS is operating on channel-1 when it is in cell-1.
- As it moves to cell-2, the MSC will assign a new channel i.e. channel-2 to it when it enters into cell-2.

4. **Inter-MSC handover :**

- The inter MSC handover has been shown in Fig. 2.11.1(d).



(GT-36) **Fig. 2.11.1(d) : Inter MSC handover in GSM**

- This type of handover takes place when a mobile station (MS), moves from one cell to the other (cell-1 to cell-2) controlled by different BSCs and different MSCs as well.
- Such a handover is performed by two MSCs together.
- This type of handover sets particularly high requirements on the cellular network.

2.12 Security in GSM :

- In the second generation digital cellular systems like GSM, the provision of security is relatively easy as compared to the first generation analog systems.
- It is possible to use the methods like encryption, scrambling, FEC etc. to ensure security in the system.
- GSM offers different security services with the help of the personal information stored in AuC and in the SIM.

Types of security services :

- GSM offers the following security services :
  1. Access control and authentication.
  2. Confidentiality.
  3. Anonymity.

2.12.1 Access Control and Authentication :

Definition :

- Authentication is the process of ensuring that the communication over the wireless radio medium is secured.
- The authentication of a user is the process of ensuring and verify that the user is really the person who claims he is.
- There are two steps in authentication process of GSM.
- In the first step the authentication of a valid user is carried out for the SIM.
- The user needs a secret PIN to access the SIM. And in the second step the authentication of the subscriber is done.

2.12.2 Confidentiality :

- The confidentiality of all the user related data is ensured by encrypting it.
- The BTS and MS apply **encryption** to voice, data and signaling information, once the authentication is done.
- Due to encryption, it is possible to apply confidentiality only between MS and BTS but not over the entire end to end GSM network.

2.12.3 Anonymity :

- In order to provide anonymity to the user, all data is first encrypted.
- The user identifiers (the information which could reveal the user's identity) is not transmitted.
- Instead a temporary identifier (TMSI) is transmitted by GSM.
- The VLR assigns this identifier newly after each location update.
- Additionally the TMSI can be changed anytime by the VLR.

2.12.4 Authentication in GSM :

Definition :

- The authentication of a user is the process of ensuring and verifying that the user is really the person who claims he is.
- Authentication is essential to ensure that the communication over the wireless radio medium is secured.
- The authentication process involves two functional entities :
  1. The SIM card in mobile phone.
  2. The Authentication Center (AUC)
- An important element that ensures security in the GSM system is the Subscriber Identity Module **(SIM) card**, which is an intelligent plastic card with a microcontroller.
- SIM is an inherent part of a mobile terminal.
- The user receives the SIM card from the network operator, which contains a list of individual user data, encryption programs and keys.
- Because it is possible to separate the SIM and the mobile phone, the SIM card provides an additional security means against an unauthorized usage of the stolen or lost phone.
- A **mobile station** consists of two parts that are strictly related to each other : a mobile phone and a SIM card.
- The SIM card contains a microcontroller with ROM, RAM and **NVM (Non-Volatile Memory).**
- The ROM stores the programs implementing A3 and A8 encryption algorithms.
- The capacity of the ROM is 4 to 6 kbits and cannot be copied.
- The RAM is very small and its storage capacity can be up to 256 bytes.
- The size of **NVM** is about 2 to 3 kB and it contains the following individual user's parameters and data :

Ki is user's authentication key,

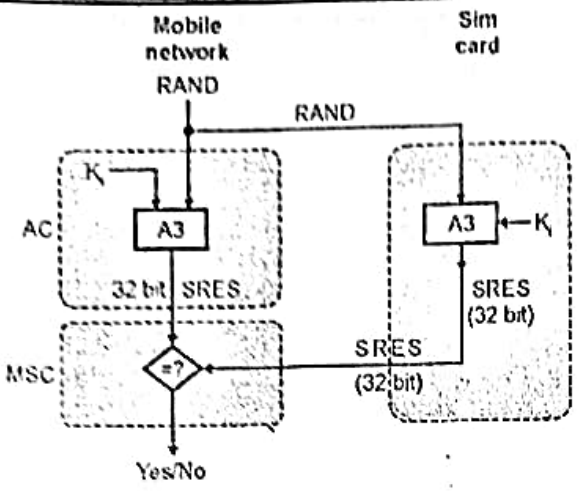
1. IMSI (International Mobile Subscriber Identity) : It is a 15-bit long user's individual identification number which consists of the country code, network code and number of the user,
2. TMSI (Temporary Mobile Subscriber Identity) : It is a temporary identification number assigned to the user after each registration in a new VLR,
3. LAI (Location Area Identifier),
4. PIN (Personal Identification Number); It is a 4 or 8-digit code identifying the user with respect to the SIM card,
5. The personal telephone book : It is a list of telephone numbers entered by the user,
6. The list of foreign cellular networks where roaming is allowed,
7. The received short messages (SMS)

- A specially designed algorithm A3 is used for carrying out authentication.
- After carrying out the authentication, a key is generated for encryption, with the help of another specially designed algorithm A8.
- GSM provides the security services by using three algorithms called **A3, A5 and A8.**
- Their functions are as follows :

Sr. No.	Algorithm	Function
1.	A3	Used for Authentication
2.	A5	Used for Encryption
3.	A8	Used for generation of cipher key.

2.12.5 Authentication Algorithm A3 :

- Authentication is done with the help of SIM. SIM stores authentication key K_i and the user IMSI.
- During the authentication process the Mobile Switching Center (MSC) or MTSO challenges the Mobile Station (MS) with a random number (RAND) which is generated by the AC (Access control) as shown in Fig. 2.12.1.



AC : Access control.
K : User's authentication key.
A3 : Authentication algorithm.

(GT-37) **Fig. 2.12.1 : Verification of the user authenticity**

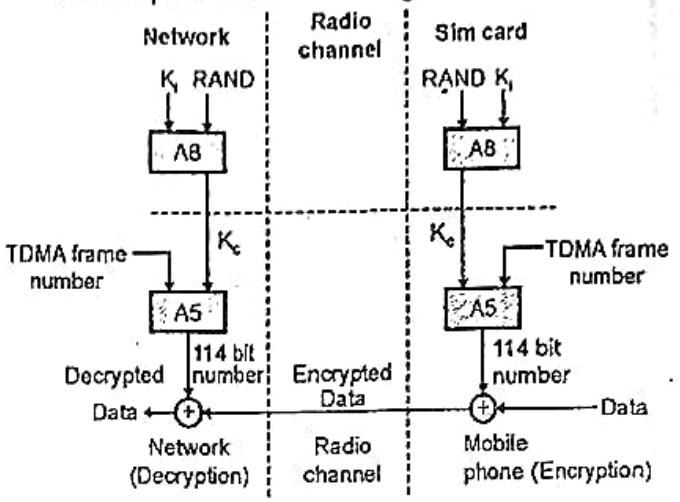
- The SIM card makes use of this RAND received from the MSC along with a secret key k_i stored within the SIM as input.
- Both RAND and k_i are basically 128 bit digital numbers.
- The A3 algorithm works on the RAND and k_i inputs to produce a 32 bit output called as the signature response (SRES).
- The SRES is then sent back to MSC from MS as the answer to the challenge. Using the same algorithm the AUC also generates a SRES.
- Then the SRES generated by MS (SIM) and AUC are compared.
- If they are identical then it is an indication that MS is an authentic user.
- That means it is concluded that SIM card is genuine.

2.12.6 Data Encryption Process using A5 and A8 Algorithm :

- Fig. 2.12.2 shows the data encryption process in GSM using A5 and A8 algorithm.
- In GSM, the A5 algorithm is used for the data encryption.
- Only manufacturers of the cellular devices have an access to this algorithm.
- The A5 algorithm is more secure because the secret key K_c is never transmitted over the air. Initially the network activates the A5 algorithm.

Encryption process :

- The data encryption process takes place at the Mobile phone as shown in Fig. 2.12.2.



(GT-38) **Fig. 2.12.2 : Data encryption process using A5 and A8**

- The SIM card initially obtains the data encryption key K_c by applying the RAND number sent by the mobile network during the process of authentication and the individual secret key K_i, to algorithm A8. The A8 algorithm is present inside the SIM card.
- Then the A5 algorithm generates a 114-bit number by using the encryption key K_c and the current 22-bit TDMA frame number.
- These 114-bits are modulo-2 added with the information (i.e. data) bits of the normal burst to produce the encrypted data.
- This encrypted data is then transmitted over the radio channel.

Decryption process :

- The data decryption process takes place at the network as shown in Fig. 2.12.2.
- The same process of generation of the encryption key Kc from the RAND and Ki and then generation of 114 bit number from Kc and the current TDMA frame number, is carried out on the network side as well using A8 and A5 algorithms.
- The received encrypted data is applied to a modulo-2 adder alongwith this 114 bit number at the network site.

- If the received data has no errors during the transmission, the modulo 2 addition of the received data and the generated encrypted data results in the original data sequence. This is the process of decryption.
- The block diagram representation of the encryption and decryption processes are as shown in Fig. 2.12.2.

2.13 GSM Services :

- The GSM services can be classified into three types of services :
  1. Teleservices
  2. Data services
  3. Bearer services
  4. Supplementary services

2.13.1 Teleservices :

- These services allows subscriber to use terminal equipment functions for communication with other subscribers.
- The teleservices support emergency calling, FAX services, Videotex and Teletex services though they are not integral part of the GSM standard.
- In other words, the standard mobile telephony and the mobile originated or base originated traffic comes under the teleservices.
- The tele-services are as follows :
  1. Digital telephony. 2. Emergency calling.
  3. SMS. 4. EMS.
  5. MMS. 6. Group 3 FAX.

1. Digital telephony :

- The main service of GSM is to provide a high quality digital voice transmission, with a minimum bandwidth of 3.1 kHz.
- Special codecs (combination of coder and decoder) are used for transmission of voice digitally.

2. Emergency calling :

- With this GSM service the same emergency number can be used throughout a country.
- This is a mandatory but free service with the highest connection priority.
- If this number is dialled, then the call with the nearest emergency center is set up automatically.

3. Short Message Service (SMS) :

- With this service the user can send messages upto 160 characters. SMS messages are not transmitted over the standard data channels of GSM.
- Instead they are sent over the unused capacity of signaling channels.
- Hence SMS sending and receiving is possible even when the voice or data is being transmitted.
- SMS can transfer logos, ring tones, horoscopes alongwith the text messages.
- It is also possible to update the software of a mobile phone via SMS.

4. Enhanced Message Service (EMS) :

- EMS is the successor of SMS which offers a message size of upto 760 characters.
- It is possible to send text, ring tones, small images, animated pictures in a standard way using EMS. But EMS service never took off commercially.

5. Multimedia Message Service (MMS) :

- With this service, it is possible to transmit large pictures (GIF, JPEG) and short video clips.
- MSS is integral part of mobile phones with an inbuilt camera.

6. Group 3 FAX :

- This is one more non-voice tele-service in which fax data is transmitted as digital data over the network of analog telephone lines.

2.13.2 Data Services :

- These services allow subscriber to transmit appropriate signals across user network interfaces.
- **Data services** are the GSM services corresponding to the communication between computers and packet switched traffic.
- It supports packet switched protocols and data rates from 300 bps to 9.6 kbps.
- New developments are going on to increase the data rate further.

- Data can be transmitted in two modes :
  1. **Transparent mode :** GSM network provides standard channel coding method for user data.
  2. **Non-transparent mode :** GSM network provides special coding methods based on particular data interface.

2.13.3 Bearer Services :

Bearer Services :

- Bearer services are basically the **data services** which correspond to the communication between a computer and packet switched traffic.
- Bearer **services** are defined as all those services that enable the transmission of data between **interfaces and networks.**
- In the classical GSM model, the bearer services are **connection oriented** and use circuit or packet switching.
- In GSM, there are different mechanisms for the data transmission.
- The **bearer services** supports the data transmission of transparent and non-transparent, synchronous or asynchronous types.
- Bearer services are of two types :
  1. Transparent bearer services.
  2. Non-transparent bearer services.

1. **Transparent bearer services :**

- These services use the functions of only the **physical layer** for the data transmission.
- The delay and the throughput of the data transmission is constant if there is no transmission error.
- The transmission quality can be improved only by using the Forward Error Correction (FEC).
- The data rates of 2.4, 4.8 or 9.6 kbps are possible depending on the FEC.
- These services do not try to recover the lost data irrespective of the cause.

2. **Non-transparent bearer services :**

- These services use the functions of the first three layers of the OSI model i.e. physical, data link layer and network layer.
- They use protocols in the DLL and network layer to add error correction and flow control.
- Due to this, a special mechanism of **selective reject** gets added to facilitate retransmission of lost or erroneous data.
- This reduces the error rate remarkably. But delay and throughput do not remain constant.
- They depend on the transmission quality.

Features of bearer services :

- The important features of bearer services are as follows :
  1. Full duplex data transmission.
  2. Synchronous transmission data rates : 1.2, 2.4, 4.8 and 9.6 kbps.
  3. A synchronous transmission data rates : 300 to 9600 bps.

2.13.4 Supplementary Services :

- These services are digital in nature and they are offered as supplements with the basic teleservices.
- The supplementary services provide various enhancements for the standard telephony services.
- Some of the typical supplementary services are as follows :
  1. **Conference Call :** This service allows a mobile subscriber to start a conference call i.e. a simultaneous conversation takes place between three or more mobile subscribers.
  2. **Call Waiting :** During a conversation this service informs a mobile subscriber about an incoming call. The user can answer, reject, or ignore the incoming call while conversation.
  3. **Call Hold :** This service allows a user to put an incoming call on hold and after a while call can be resumed.

4. **Call Forwarding :** To divert calls from the original recipient to another number call forwarding service is used. The user himself can set up this service on his/her mobile.
5. **Call Barring :** To restrict some type of calls such as outgoing calls like ISD or incoming calls from unwanted numbers call Barring service is useful.
6. **Caller Identification :** On your mobile screen, this service displays the telephone number of the person who is calling. It displays telephone number of a person to whom you are connected.
7. **Suggestion of Charge :** This service informs the user about the cost of the services used by them.
8. **Closed User Groups :** This service is intended for the group of subscribers who want to call only each other in the group.

2.14 Mobility Management in GSM :

- One of the major function of a GSM network is Mobility management which allows mobile phones to work.
- The goals of mobility management in GSM are :
  1. To track the location of subscribers.
  2. To allow calls, SMS and other mobile phone services to be delivered.

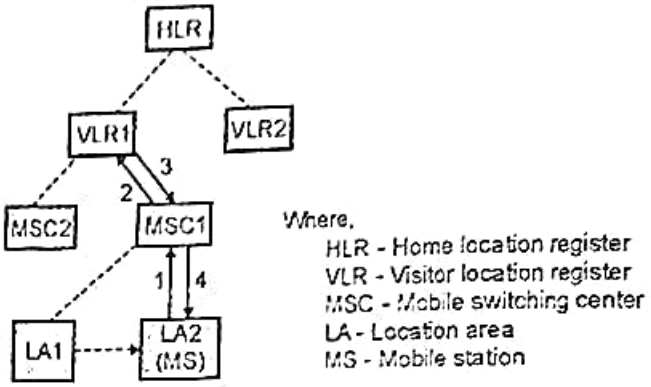
2.14.1 GSM Location Management :

- The location update procedure in GSM occurs when the MS (Mobile station) moves from one LA into another area.

2.14.2 Basic Location Update Procedure :

- The basic location update procedure handles following movements without considering fault tolerance and VLR overflow :
  1. Inter-LA movement
  2. Inter-MSC movement
  3. Inter-VLR movement

1. **Inter-LA Movement :**
- In this case, the MS moves from a LA1 to LA2. Here both the LAs are connected to the same MSC (Mobile station controller) as shown in Fig. 2.14.1(a).
- Fig. 2.14.1(a) shows the steps in Inter-LA movement registration within the same MSC.



(G-2630) **Fig. 2.14.1(a) : Inter-LA movement registration within the same MSC**

Steps involved :

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update request is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e. MAP_UPDATE_LOCATION_AREA.

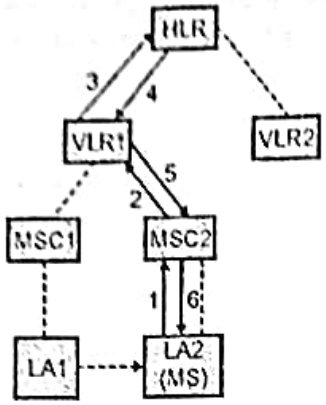
This message consists of the address of the MSC, TMSI of the MS, Previous location area identification (LAI), ID for LA1 and LA2 and other related information.

Step 3 : The VLR observes that LA1 and LA2 belongs to the same MSC.

Step 4 : VLR updates LAI (local area identification) field of VLR record and replies with an acknowledgement MAP_UPDATE_LOCATION_AREA_ACK to the MS via MSC.

2. **Inter-MSC Movement :**
- In this case LA1 and LA2 belongs to different MSCs having the same VLR as shown in Fig. 2.14.1(b).

Fig. 2.14.1(b) shows the steps in Inter-MSC movement registration.



(G-2631) **Fig. 2.14.1(b) : Inter-MSC movement registration**

Steps involved :

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update message is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e. **MAP_UPDATE_LOCATION_AREA.**

This message consists of the address of the MSC, TMSI of the MS, Previous location area identification (LAI), ID of LA1 and LA2 and other related information.

Step 3 : The VLR observes that previous LA and target LA belongs to different MSCs i.e. MSC1 and MSC2 respectively which are connected to the same VLR. The HLR address of the MS is obtained from the MS's IMSI which is stored in VLR record. VLR sends

MAP_UPDATE_LOCATION message to the HLR which includes IMSI of MS, address of MSC2 and VLR1 and other related information.

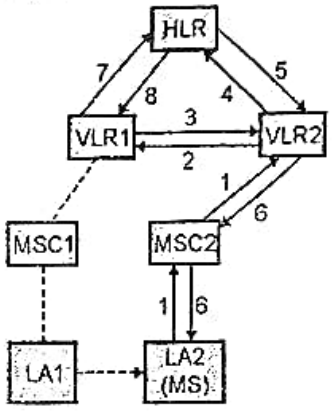
Step 4 : The HLR identifies the MS's record by using the received IMSI and updates MSC address in the record. HLR replies with an acknowledgement to the VLR.

Step 5 : The VLR observes LA1 and LA2.

Step 6 : VLR updates LAI (local area identification) field of VLR record and replies with an acknowledgement **MAP_UPDATE_LOCATION_AREA_ACK** to the MS via MSC.

3. Inter-VLR Movement :

- In this case LA1 and LA2 belongs to different MSCs having different VLRs as shown in Fig. 2.14.1(c).
- Fig. 2.14.1(c) shows the steps in Inter-VLR movement registration.



(G-2632) **Fig. 2.14.1(c) : Inter-VLR movement**

Steps involved :

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update message is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e. **MAP_UPDATE_LOCATION_AREA.**

This message consists of the address of the MSC, TMSI of the MS, Previous location area identification (LAI), ID of LA1 and LA2 and other related information.

Step 3 : As the Mobile Station moves from VLR1 to VLR2, VLR2 do not have the VLR record and IMSI of the MS. VLR2 identifies the address of VLR1 from the message **MAP_UPDATE_LOCATION_AREA.**

VLR2 sends **MAP_SEND_IDENTIFICATION** message to VLR1.

Step 4 : The HLR identifies the MS's record by using the received IMSI and updates MSC address in the record. HLR replies with an acknowledgement to the VLR containing the TMSI of the MS. VLR1 uses this TMSI to find the corresponding IMSI in the database. This IMSI is then sent back to VLR2.

Step 5 : The VLR2 generates a VLR record of the MS. It sends registration message for the updating the HLR. HLR updates the record of MS and sends acknowledgment back to the VLR2.

Step 6 : VLR2 creates a new TMSI and sends it to the MS.

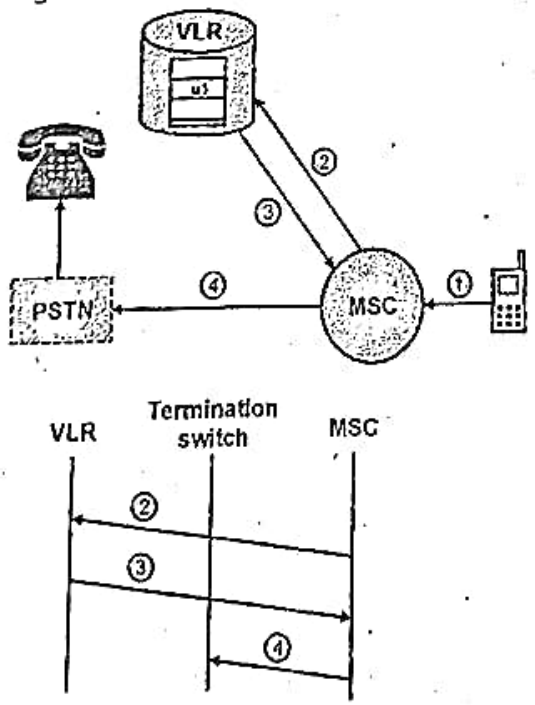
Steps 7 & 8 : The outdated record of MS in the VLR1 is deleted.

2.14.3 GSM Transaction Management :

- The concepts of call origination and termination procedures and algorithms are explained as follows.

1. Basic Call Origination Procedure :

- Fig. 2.14.2 shows the basic call origination process.



② MAP_SEND_INFO_FOR_OUTGOING_CALL
③ MAP_SEND_INFO_FOR_OUTGOING_CALL_ack
④ IAM

(G-3057) **Fig. 2.14.2 : Call origination operation**

- The algorithm for the basic call origination Procedure is described in the following steps :

Step 1 : The MS of user 1 i.e. MSu1 sends the call origination request to the MSC.

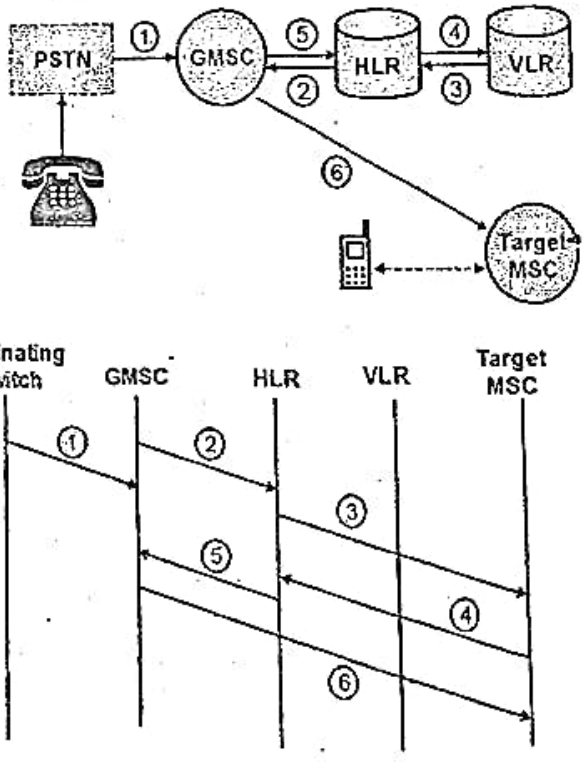
Step 2 : The MSC forwards the request of MSu1 to the VLR by sending the message MAP_SEND_INFO_FOR_OUTGOING_CALL.

Step 3 : The VLR checks the u1's profile in the database and sends the acknowledge message MAP_SEND_INFO_FOR_OUTGOING_CALL_ACK to the MSC to grant the call request of u1.

Step 4 : According to the standard PSTN call setup procedure, the MSC sets up the trunk.

2. Basic Call Termination Procedure :

- Fig. 2.14.3 shows the basic call termination process.



① ISUP IAM
② MAP_SEND_ROUTING_INFORMATION
③ MAP_PROVIDE_ROAMING_NUMBER
④ MAP_PROVIDE_ROAMING_NUMBER_ack
⑤ MAP_SEND_ROUTING_INFORMATION_ack
⑥ ISUP IAM

(G-3058) **Fig. 2.14.3 : Call termination operation**

- As shown in Fig. 2.14.3, the routing information is obtained from the serving VLR for call termination to a GSM subscriber.
- The algorithm for the basic call termination procedure is described in the following steps :

Step 1 : When PSTN user dials the mobile station ISDN number (MSISDN), the call is routed to a gateway MSC by an SS7 ISUP IAM message.

Step 2 : In order to obtain the routing information, the gateway MSC or ISDN exchange interrogates the HLR by sending **MAP_SEND_ROUTING_INFORMATION** to the HLR. This message includes the MSISDN of the MS and other related information.

Step 3 : To obtain the mobile subscriber roaming number (MSRN), the HLR sends a message **MAP_PROVIDE_ROAMING_NUMBER** to the VLR.

This message includes the IMSI, the MSC number, and other related information. During the location update, the MSC number is maintained in the HLR at inter-MSC and inter-VLR location update. MSC number is used to set up the voice trunk and it provides the address of the target MSC.

Steps 4 and 5 : The VLR generates the MSRN by using the MSC number. MSC number is stored in the VLR record of the MS. This roaming number is sent back to the GMSC via the HLR.

Step 6 : The MSRN provides the address of the target MSC residing the MS. To set up the voice trunk, an SS7 ISUP IAM message is directed from the GMSC to the target MSC.

- The location information in HLR or VLR is utilized in the location update and the call-delivery procedures.
- In case of failure of the mobility database, the system will not be able to track the MS.

2.14.4 Advantages of GSM :

- Following are the advantages of GSM :

1. GSM provides better quality of speech.
2. Data transmission is supported in the GSM system.
3. International roaming is possible in the GSM.
4. New services are provided due to ISDN compatibility.
5. There is a large variety of mobile phones, which operate on GSM.
6. The working of phone is based on a SIM card and hence user can change the different variety of phones.
7. The power consumption is less in GSM mobiles.
8. It is more cost effective.

2.14.5 Disadvantages of GSM :

- Following are the disadvantages of GSM :

1. Main disadvantage of GSM is that many users share the same bandwidth, which may result in the transmission interference.
2. As compared to CDMA, the per-unit charge on roaming calls is higher in GSM.

2.14.6 Applications of GSM :

- Following are a few other applications of GSM :

1. Educational institutions and organizations
2. Managing traffic
3. Bus / railway station
4. Business
5. Medical field
6. Mobile telephony
7. Telemetry system
8. Toll collection
9. Forest fire and rainfall detection systems
10. Health monitoring
11. Weather forecasting.

2.15 GPRS - General Packet Radio Service :

- GPRS is a packer based technique which could be the next step in evolution of GSM as well as IS-136 and PDC standards (all the TDMA based 2G standards).

Principle :

- GPRS operates by supporting a multiple user network sharing of individual channels and time slots.
- This is different than the principle of HSCSD. Due to this technique, GPRS can support many more users than HSCSD but in a burst manner (non-continuous manner).
- The GPRS standard provides a packet network on dedicated GSM or IS-136 radio channels.

Air interface :

- The modulation formats specified in the original 2G TDMA standards (GSM and IS-436) are retained in GPRS. But it uses a completely redefined air interface (as compared to GSM or IS - 136) for better handling of data.
- GPRS has dedicated radio channels and particular time slots that allow an always on access to the network.
- The GPRS subscribers are instructed automatically, to tune to the above mentioned channels and time slots.

Uplink and downlink frequencies :

- The uplink and downlink frequencies used in GPRS are exactly same as those used in GPS .

Uplink	890 – 915 MHz
Downlink	935 – 960 MHz

Data rates :

- If all the eight time slots of a GSM channel are dedicated to GPRS, it is possible for an individual user to achieve a data rate of 171.2 kbps.
- However these data rates decrease with increase in the number of users trying to use the GPRS network.
- The data rate specified by GPRS (dedicated peak) i.e. 21.4 kbps per channel operates well with both GSM and IS-136 and has been successfully implemented.
- There are eight time slots of a GSM radio channel. When all of them are dedicated to GPRS, a user can achieve a data rate of $8 \times 21.4 = 171.4$ kbps.

Error correction :

- In GPRS the applications are required to provide their own error correction schemes.

GPRS Implementation :

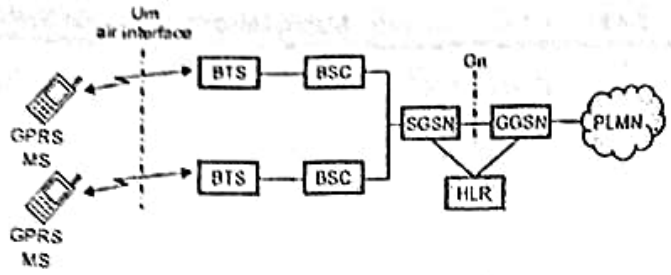
- For implementation of GPRS, the GSM operator needs to install only the new routers and gateways at the base station.
- A new software that redefines the base station air interface and time slots, is also needs to be installed at standard the base station.
- A new RF base station hardware is also required.

2.15.1 Features of GPRS :

1. Channel bandwidth : 200 kHz.
2. Duplex : FDD.
3. No new spectrum is required.
4. Old GSM handsets cannot be used. Needs new GPRS handsets.
5. It is built on the existing GSM network to provide high-speed data service.
6. GPRS has dedicated radio channels and particular time slots that allow an always on access to the network.
7. High data rate up to 171.2 kbps for a single user.
8. GPRS supports both point-to-point and point-to- multipoint packet service.
9. GPRS is designed to support bursty applications like email, traffic telematics, telemetry, broadcast services and web browsing.
10. GPRS provides the following security services : Authentication, access control, user information confidentiality and user identity security.

2.15.2 GPRS Architecture :

- Fig. 2.15.1 shows the architecture of the GPRS system.



(GT-48) **Fig. 2.15.1 : Architecture of GPRS system**

- In GPRS two new network elements are introduced, which are known as GSN (GPRS support nodes).
- Fig. 2.15.1 shows GPRS architecture, which is formed with all GSNs, which are integrated into the standard GSM architecture, alongwith some interfaces.

GPRS support nodes :

- There are two types of support node in GPRS :
  1. SGSN (Serving GPRS support node)
  2. GGSN (Gateway GPRS support node).

1. Serving GPRS Support Node (SGSN) :

- As shown in Fig. 2.15.1, the BSCs are connected to SGSN which acts as the service access point to the GPRS network, for the GPRS user.
- SGSN is analogous to MSC in the GSM networks. We may view it as a packet switched MSC.
- Within the service area of SGSN, it delivers packets to MS (mobile stations).
- SGSNs send queries to home location registers (HLRs) for obtaining the profile data of GPRS subscribers.
- In their service area, SGSNs detect new GPRS MS and process the registration of new mobile subscribers and keep records of their locations inside a given area.
- In this way the SGSNs perform the **mobility management functions** such as attaching/detaching a mobile subscriber and its location management.

Functions of SGSNs :

- The main functions of SGSN are as follows :
  1. Routing of data to and from mobile station.
  2. To handle authentication.
  3. To carry out data compression and ciphering.
  4. Tracking of location and mobility administration.
  5. Stores the location and profile of users.
  6. Mobility management.

2. Gateway GPRS Support Node (GGSN) :

- The GGSNs are connected to the external packet switching data networks, like the X.25 or the Internet as shown in Fig. 2.15.1.
- For all these networks the GGSNs acts simply as a router.
- When the data addressed to a specific mobile user is received by a GGSN, it first checks if the called address is active.
- If it is active, then the GGSN forwards the data packets to SGSN.
- However if the called address is found inactive, then GGSN simply discards the received packets.
- The GGSNs route the mobile originated data packets to the desired network.
- They also track the mobile user in association with the SGSNs.

3. GPRS Interfaces :

- The GPRS architecture includes signaling interfaces with various protocols, which controls and support the transmission of packets across the networks and to the mobile stations.
- Following are the GPRS interfaces :
  1. Air Interface (Um) : It connects MS and BTS (Base transceiver station).
  2. A-bis Interface : It connects BTS and BSC (Base station controller).
  3. Gb Interface : It connects BSC with SGSN.
  4. Gn Interface : It connects SGSN and GGSN.
  5. Gi Interface : It connects GGSN with external PDN (Packet Data Network).
  6. Gr Interface : It connects SGSN and HLR. Exchange the user information between SGSN and HLR.

7. Gc Interface : It connects GGSN and HLR. Exchange the location information between GGSN and HLR.

2.15.3 GPRS Radio Interface :

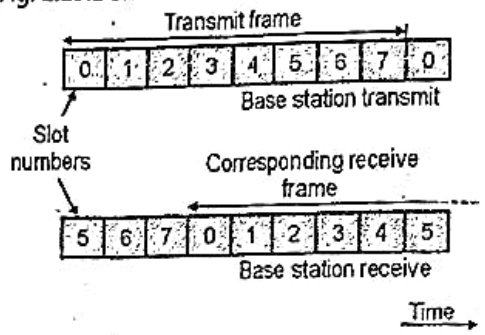
- The GPRS radio interface has to accommodate GSM voice as well as packet data and this requires updates including to the slot & burst.
- One requirement for GPRS was that it would be able to operate alongside the GSM system with mobiles for both types being able to access the radio access network.

GPRS modulation scheme :

- GPRS builds on the basic GSM structure. It uses the same signal format having 200 kHz channel bandwidths.
- It also has the same modulation scheme and using GMSK modulation.
- Retaining the same modulation scheme means that the level of upgrade required to be able to support GPRS in addition to GSM is minimised.
- GMSK modulation was chosen for GSM originally because it offered a number of advantages including good spectral efficiency, resilience to interference, low levels of interference outside the wanted bandwidth, and the ability to use a non-linear RF power amplifier.
- This last point is of great importance because the use of a non-linear power amplifier brings greater levels of efficiency and this results in longer battery life - an important factor for mobile phones.

GPRS frame and slot structure :

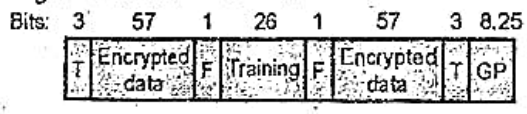
- Again the GRPS air interface employs the same basic structure as that adopted for GSM.
- The overall slot structure for this channel is the same as that used within GSM, having the same power profile, and timing advance attributes to overcome the different signal travel times to the base station dependent upon the distance the mobile is from the base station.
- This enables the burst to fit in seamlessly with the existing GSM structure.
- GPRS employs four levels of error correction in its data encoding.
- The level of error correction used depends upon a number of variables and it is defined as four levels, CS1, CS2, CS3, and CS.
- Fig. 2.15.2 shows the frame structure of GPRS.



(G-2730) **Fig. 2.15.2 : Frame structure of GPRS**

GPRS burst structure:

- Fig. 2.15.3 shows the burst structure of GPRS.



(G-2731) **Fig. 2.15.3 Burst structure of GPRS**

- Each GPRS burst of information is 0.577 ms in length and is the same as that used in GSM.
- The GPRS burst carries two blocks of 57 bits of information in line with a GSM burst, giving a total of 114 bits per burst.
- It therefore requires four GPRS bursts to carry each 20 ms block of data, i.e. 456 bits of encoded data.
- Slots can be assigned dynamically by the BSC to GPRS dependent upon the demand, the remaining ones being used for GSM traffic.
- Where :

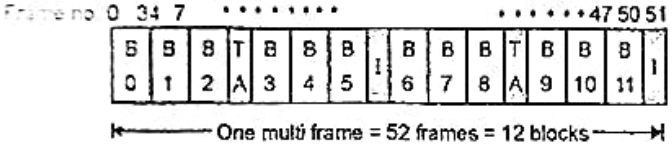
  T = tail bit and F = coding flag

- The BSC assigns PDCHs to particular time slots, and there will be times when the PDCH is inactive, allowing the mobile to check for other base stations and monitor their signal strengths to enable the network to judge when handover is required.

- The GPRS slot may also be used by the base station to judge the time delay using a logical channel known as the Packet Timing Advance Control Channel (PTCCT).
- The GPRS radio interface is very similar to that of GSM and this enables both GSM and GPRS to operate via the same radio access network.
- They can operate together on the same carrier, bursts of GSM and GPRS occupying the same frame.
- This enabled GPRS to be an evolution of GSM and base stations to steadily have GPRS incorporated into them.

2.15.4 GPRS Frame Structure and Channel Coding :

- Fig. 2.15.4 shows the structure of a GPRS multiframe.



(GT-50) **Fig. 2.15.4 : GPRS multiframe structure**

- It can be seen that, four subsequent frames constitute a block.
- A block is a unit prepared from the point of view of the applied channel coding.
- There are 12 such blocks in the multiframe (B0-B11).
- One multiframe corresponds to 52 frames or 12 blocks. Out of the remaining four frames, two frames are idle(I) frames and two other frames (TA) are used to update the frame timing advance.
- As we know, a single GSM normal burst carries 114 bits of user data.
- Therefore, one block in a GPRS frame, consisting of 4 frames contains 4 x 114 = 456 bits.
- Therefore each coding scheme applied in GPRS produces a 456-bit block.

1 multiframe = 52 frames = 12 blocks (B0-B11)

1 block (1 unit) = 4 subsequent GSM bursts = 4 frames

1 GSM burst = 114 bits, therefore 1 block = 4 GSM bursts × 114 bits = 456 bits.

Channel coding :

- Channel coding adds redundant bits to protect the transmitted data packets against errors.
- The channel coding methods used in GPRS is same as that in standard GSM systems.
- GPRS uses a two level channel coding. The two levels are called as the outer coding and the inner coding levels.
- The outer level code is a block code which adds a few tail bits at the end of the code word.
- Then this code word is coded using convolutional codes and some bits are punctured to produce a 456 bit code word.
- The coding scheme is decided based on channel conditions and service requirements.
- Coding schemes decide the quality of service of the GPRS system, which also depends on the reliability, delay, priority of service and throughput.

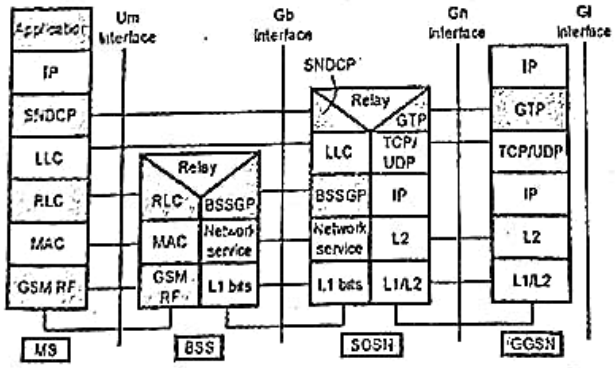
2.15.5 GPRS Transmission Management :

- Before GPRS transmission starts, it is necessary to perform some special procedures so as to make the mobile station and network ready for data exchange.
- First step in this procedure is that, a mobile station should **register with the SGSN** serving the area in which the mobile station is located. Such a procedure is called **GPRS Attach.**
- After this the network carries out the user authorization, sends the user profile from the HLR to the SGSN and finally assigns a Packet Temporary Mobile Subscriber Identity to the user.
- For certain types of MS the combined GSM/GPRS registration can be performed,
- Note that the MS is not visible in the GPRS network and is in the idle state before performing GPRS Attach procedure.

- After the network attachment, the MS switches to the ready state and it sends information to the SGSN after every movement to a new cell.
- Therefore, the location of the MS in the ready state is known very accurately.
- A MS in the ready state can send and receive packets if initiation of the data exchange is done.
- A mobile station goes in standby mode, if the it does not send or receive packets for some time.
- The location of the MS in the standby state also is traced very accurately.
- SGSN keeps track on the location of the MS and it is ready to send or receive packets.
- But if it does not participate in data exchange then it goes into standby mode.
- The location of the MS in standby mode is tracked by cell group RA (routing area). For this paging is required.
- PDP address (Packet Data Protocol) : For data exchange with IP or X.25 network, MS needs special address called as PDP address.
- It is unique for each session. It consists of PDP type, PDP address, requested QoS and address of GGSN. This is stored in MS, SGSN and GGSN.

2.15.6 GPRS Protocol Stack / GPRS Protocol Reference Model :

- Fig. 2.15.5 shows GPRS protocol stack for the user data transmission.



(G-2427) **Fig. 2.15.5 : GPRS transmission plane protocol stack**

- Um (air interface) is located between MS and BSS, the Gb interface is located between BSS and SGSN and Gn interface is located between SGSN and GGSN.
- SNDCP (Subnetwork dependant convergence protocol) encapsulates the IP packets in GPRS specific packet format which is used between SGSN and MS.
- LLC layer provides a reliable logical link to the data units from the higher layers, which depends on the underlying radio interface protocols.
- LLC provides either acknowledged or unacknowledged data transmission.
- GTP (GPRS tunneling protocol) tunnels user data between the two GSNS in the GPRS backbone network.
- BSSGP (base station subsystem GPRS protocol) layer conveys routing and QoS related information between the BSS and SGSN.
- RLC (Radio Link Control) protocol provides reliable radio link for the data transfer between MS and BSS.
- MAC layer controls the multiplexing of signaling and data messages from various GPRS users.
- GSM RF (Radio Frequency) layer controls the physical channel management, modulation / demodulation, transmission, power control and channel coding / decoding.

2.15.7 GPRS Services :

- Data transfer in a GPRS system is performed within the selected bearer or supplementary services.
- The bearer services can be divided into two categories :

1. **The Point-to-Point (PTP) Service :**

- It is a connection between two individual users, which can be realized in either a connectionless mode (using the IP network) or a connection-oriented mode (using the X.25 network) and

2. **The Point-to-Multipoint (PTM) Service :**

- It is a connection between one user and a specified number of other users.
- It is possible to select the users their location in a specified area (multicast service) or can be addressed according to a specified list (group service).

Bearer Services in GPRS :

- Bearer services of GPRS offers End-to-End packet switched data transfer services.
- A GPRS supports the two types of data transfer services such as PTP (point-to-point) and PTM (point-to-multipoint) services.
- Now a day, the Point-to-Point (PTP) service is available and in the future releases of GPRS PTM will be available.
- The types of data services supported by GPRS are as follows :
  1. **SMS (Short message service) :** GPRS supports SMS as a data bearer service. SMS offers text messages.
  2. **MMS (Multimedia messaging service) :** GPRS supports MMS, which offers multimedia messages. Audio, pictures, clips or videos can be sent via MMS.
  3. **WAP (Wireless application protocol) :** GPRS supports WAP, which is a data bearer service over HTTP protocol.

2.15.8 Characteristics of GPRS :

- Following are the characteristics of GPRS :
  1. GPRS uses packet switched network.
  2. It uses GSM architecture and GPRS support nodes.
  3. It enables voice and data flow through the network.
  4. It has dynamic time slot allocation.
  5. It is faster than GSM and code division multiple access (CDMA).

2.15.9 Advantages of GPRS :

- Following are the advantages of GPRS :
  1. **Speed :** GPRS technology offers higher data rate than GSM. GPRS provides speed limit upto 171 kbps and offers throughput upto 40 kbps.
  2. **Packet switched :** GPRS is packet switched system circuit and parallely packet switching can be used.
  3. **Always on :** GPRS provides "Always on" capability.
  4. **Spectral efficiency :** Because of shared use of radio channels, GPRS provides a better traffic management and it has service access to a greater number of users.
  5. **Packet transmission :** For long data packet transmission GPRS works more efficiently.

2.15.10 Disadvantages of GPRS:

- Following are the disadvantages of GPRS :
  1. As GPRS uses the GSM band for data transfer, when a connection is active, calls and other network related functions cannot be used.
  2. Depending on the individual service provider GPRS is usually to be paid per Mbytes or kbytes. But this has been modified in various places where there is no more charge of per usage of GPRS downloads instead GPRS downloads are rather unlimited with a flat fee to be paid every month.
  3. It does not provide store and forward service therefore if the MS is not available the data gets lost.

2.15.11 Applications of GPRS:

- Following are the applications of GPRS :
  1. Sending and receiving e-mail, Short Message Service (SMS), Multimedia Message (MMS), fax etc.
  2. Internet access and video conference.
  3. Provides location based services.
  4. Provides the connection with PC's and other devices.
  5. Non-real time Internet applications.
  6. Retrieval of e-mails, faxes.
  7. Asymmetric web browsing (more downloading and less uploading).

2.15.12 Comparison of GSM and GPRS :

- Table 2.15.1 gives the comparison between GSM and GPRS.

Table 2.15.1 : Comparison of GSM and GPRS

Sr. No.	Parameter	GSM	GPRS
1.	Abbreviation	Global system for mobile communication	General packet radio service
2.	Based system	TDMA	GSM
3.	Users per channel	8	8
4.	Type of connection	Circuit switched technology	Packet switched technology
5.	Frame duration	4.6 ms	4.6 ms
6.	Carrier size	200 kHz TDMA	200 kHz
7.	Multiple access	TDMA	TDMA
8.	Data rates	9.6 kbps	14.4 – 171.2 kbps
9.	Frequency separation	45 MHz	45 MHz

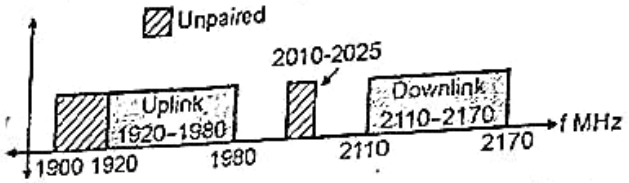
2.16 Universal Mobile Telecommunication Service (UMTS) or W-CDMA :

Objectives of W-CDMA / UMTS :

- The objectives of W-CDMA/UMTS are as follows :
  1. High frequency spectrum efficiency.
  2. Use of frequency band : 1885 MHz – 2025 MHz, 2110 MHz – 2200 MHz.
  3. Within a frequency band radio-resource should be flexible to many networks and traffic types.
  4. Radio bearer capability of up to 2 Mbps data rates.
  5. Global and seamless radio coverage can be achievable.
  6. UMTS user number is not dependent on service provider.
  7. Into a single system and one equipment services such as office, residential and cellular can be integrated.
  8. Provides flexibility for addition of new services and technical capabilities.
  9. Provides low cost services and user devices.
  10. Good quality of speech and service.

UMTS Spectrum :

- Frequency allocation used by UMTS/W-CDMA system is as shown in Fig. 2.16.1.



(G-2550) **Fig. 2.16.1 : Frequency allocation for UMTS**

- Frequency spectrum : Uplink 1920 MHz-1980 MHz, Downlink 2110 MHz-2170 MHz

2.16.1 Features of UMTS :

- The key features of UMTS are as follows :
  1. It is a wideband DS-CDMA system.
  2. It has backward compatibility with GSM.
  3. Packet data rate on downlink : 2.048 Mbps.
  4. Minimum forward channel bandwidth : 5 MHz.
  5. Frame structure : 16 slots per frame.

2.16.2 UMTS Releases and Standards :

- Release 99 or R99 is the initial release of the UMTS.
- New radio access technologies UTRA FDD and UTRA TDD are described by this release of the specification.
- Due to this the cost effective migration from GSM to UMTS takes place.
- This release was finalized in the year 1999 hence the name R99.
- Release 2000 or R00 came into existence after R99. But 3GPP realized in September 2000 that it will be impossible to finalize this standard upto the end of year 2000.

- Hence as decided by 3GPP, R2000 is divided into two standards:
  1. Release 4 (Rel-4) 2. Release 5 (Rel-5)
- For R99 all standards starts with 3.x.y whereas versions Rel-4 and Rel-5 starts with 4.x.y and 5.x.y respectively.

Release 4 :

- In the fixed network **Release 4** initiates quality of service, several execution environments and new service architectures.
- TD-SCDMA as low chiprate option to UTRA-TDD was added (i.e. only 1.28 Mchip/s that needs only 1.6 MHz bandwidth) due to the Chinese proposal.
- This release was frozen in March 2001 which already includes more than 500 specifications.

Release 5 :

- Release 5 defines basically a different core network.
- The networks based on the GSM/GPRS will be replaced by all an IP core. However, there is no change in the radio interfaces.
- IP based multimedia services (IMS) are incorporated by this standard which is under the control of the IETF's session initiation protocol.
- HSDPA (high speed downlink packet access) with speed 8-10 Mbit/s was added and a wideband 16 kHz AMR code was also added for better audio quality.
- This provides additional features such as end to end QoS messaging and many data compression mechanisms.

2.16.3 Features of UMTS Standards :

Features of Release 99 (December 99) :

1. Basic compatibility of UTRA (W-CDMA FDD).
2. Improved call control.
3. Advanced QoS for UMTS.
4. UTRAN architecture.

Features of Release 4 (March 2001) :

1. Compatibility of UTRA (W-CDMA TDD).
2. UTRAN architecture.
3. Introduced 1.28 Mchip/s TDD mode.
4. Location service.

Features of Release 5 (March 2002) :

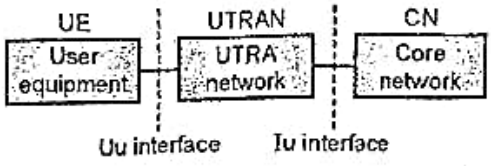
1. IMS (IP multimedia service subsystem), are incorporated.
2. HSDPA (High speed data packet access), is added.
3. Provides End to end quality of service.
4. Wideband AMR, is added for better audio quality.
5. Security enhancements.
6. Provides many data compression mechanisms.

2.16.4 Services Provided by 3G Systems / UMTS :

1. **Voice :** 3G system will provide good speech quality as compared to the telephone network.
2. **Messaging :** E-mail attachments are allowed in 3G system.
3. **MMSC multimedia messaging services :** 3G supports MMS which are designed for rich text, icons, logos, animated clips etc.
4. **Medium multimedia :** In 3G system, for web surfing, games, location based maps its downstream data rate is suitable.
5. **Interactive high multimedia :** 3G supports for this service which is used for high quality videophones, videoconferencing etc.

2.17 UMTS Architecture :

- In this section we will discuss initial UMTS standard i.e. R99.
- The simplified UMTS reference architecture is as shown in Fig. 2.17.1(a) which supports both UTRA solutions i.e. 3GPP and CDMA 2000.



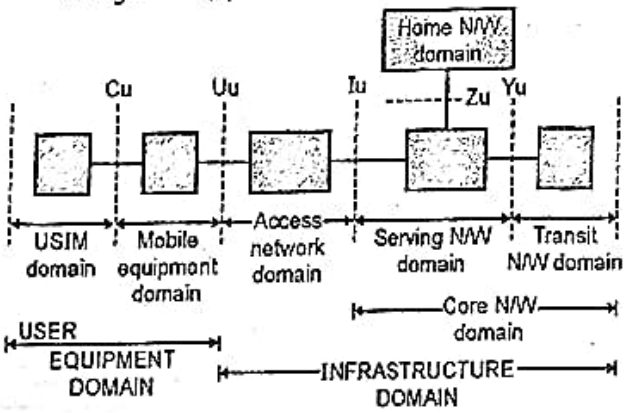
(G-2457) **Fig. 2.17.1(a) : Main components of UMTS**

Main components of UMTS :

- As shown in Fig. 2.17.1(a), the main components of UMTS are :
  1. UE (User equipment).
  2. UTRAN (UTRA network).
  3. CN (Core network).
- The UTRAN (UTRA Network) includes RNS (Radio network subsystems) and UTRAN handles call level mobility.
- The RNS performs functions such as radio channel ciphering / deciphering, handover control, radio resource management etc.
- Through the radio interface (Uu) the UTRAN is connected to user equipment (UE).
- Radio interface Uu is equivalent to the Um interface in GSM.
- The Core Network (CN) has functions such as gateways to other networks, intersystem handover etc.
- The communication between CN and UTRAN is performed via Iu interface.
- In between UE and UTRA if there is no dedicated connection then CN performs the function of location management.

2.17.1 UMTS Domain and Interfaces :

- This basic architecture of UMTS is again subdivided into **domains** and interfaces as shown in Fig. 2.17.1(b).



(G-2458) **Fig. 2.17.1(b) : UMTS domain and interface**

UMTS domains :

- As shown in Fig. 2.17.1(b), the UMTS architecture is divided into two domains :
  1. User equipment domain.
  2. Infrastructure domain.

1. User equipment domain :

- This domain is assigned to a single user and it includes functions required to access UMTS services.
- User equipment domain is again subdivided into :
  1. Mobile equipment domain.
  2. USIM (User services identity module) domain.
- For UMTS, the **USIM domain** contains the SIM which performs tasks such as encryption and authentication of users and it stores all required user related data for UMTS.
- For an enhanced program execution environment the USIM domain contains a microprocessor and USIM belongs to the service provider.
- **Mobile equipment domain** itself is end service in which functions for user interfaces as well as for radio transmission are included.

2. Infrastructure domain :

- The infrastructure domain is shared among all the users because it offers UMTS services to all accepted users.
- Infrastructure domain is subdivided into two domains:
  1. Access network domain.
  2. Core network domain.
- Access network domain includes RAN (Radio Access Networks) whereas function that are independent of access network are included in the core network domain.
- The core network domain is again divided into :
  1. Serving network domain.
  2. Home network domain.
  3. Transit network domain.

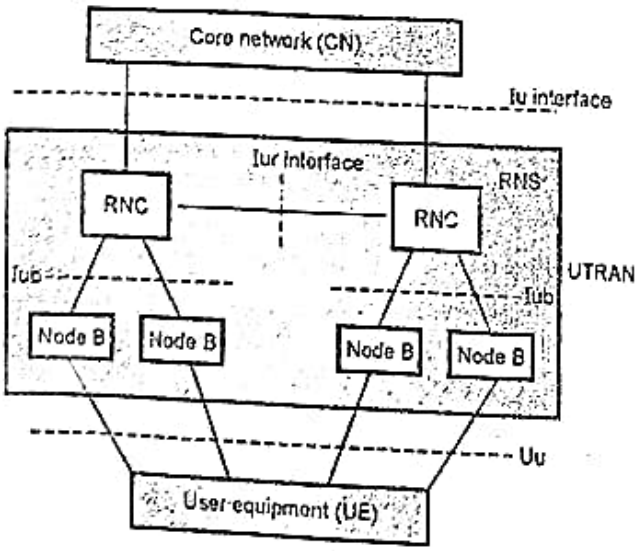
- The **serving network domain** includes all the functions used by users to access UMTS services.
- The **home network** domain performs all home network related functions of a user such as user data look-up.
- If the serving network and home network cannot contact directly then the **transit network domain** is required, to be used.

UMTS Interfaces :

- The interface points used in the UMTS architecture are :
  1. **Cu** : Interface between USIM and mobile equipment domain.
  2. **Uu** : Interface between user equipment and infrastructure domain.
  3. **Iu** : Interface between access and serving network domain.
  4. **Yu** : Interface between serving and transit network domain.
  5. **Zu** : Interface between serving and home network domain.

2.17.2 UTRA-Network (UTRAN) Architecture :

- The basic architecture of UTRAN is as shown in Fig. 2.17.2.



(G-2464) **Fig. 2.17.2 : UTRAN architecture**

Components of UTRAN :

- The two components of UTRAN are :
  1. RNS (Radio Network Subsystem).
  2. Node B.
- UTRAN architecture consists of many **RNS (Radio Network Subsystem)** controlled by **RNC (Radio Network Controller)** and includes many **node B** components as well.
- In UMTS, RNC and node B are similar to BSC and BTS respectively in GSM. Antennas which makes a radio cell are controlled by **node B**. UE (mobile device) is connected to one or more antennas.
- Through the interface Iu the core network is connected to RNC and RNC is connected to Node B through Iub interface Iur is the interface through which two RNCs are connected to each other.

Radio Network Controller (RNC) :

- The functions of RNC are as follows :

1. **Call admission control :**
   - Within each cell the RNC computes the traffic and decides whether to accept or not the additional transmissions.
2. **Encryption / decryption :**
   - Before the transmission over the wireless link the RNC encrypts all information which comes from the fixed network and vice versa.
3. **Congestion control :**
   - Many stations share the radio resources available during packet oriented data transmission.
   - In a cyclic fashion the RNC allocates bandwidth to every station by considering the QoS requirements.
4. **Radio resource control :**
   - RNC controls radio resources of the cells which are connected through a node B.
5. **Protocol conversion, ATM switching & multiplexing :**
   - ATM is the base of connection between RNCs, Node B and CN.
   - The RNC needs to switch the connections to multiplex different data streams.

6. **Setup and release of radio bearer :**

- The function of RNC is to setup, maintain and release a logical data connection to a user equipment (UE).

7. **Allocation of code :**

- The RNC selects the CDMA codes used by a UE.

8. **Management :**

- The RNS provides interfaces to the tasks such as information regarding the current load, error states, current traffic required for the network operators.

9. **Power control :**

- A relatively loose power control is performed by the RNC. It controls transmission power is based on the interference values from other RNCs or other cells.

10. **RNS location and handover control :**

- Whether another cell is better suited for a certain connection or not is decided by RNC depending on the strength of signal received by UEs or node B.
- If handover is decided by RNC it informs the new cell an UE.
- If a UE moves Out of the range of one RNC then, a new RNC has to be selected which takes responsibility of the UE. This is known as **relocation.**

Node B :

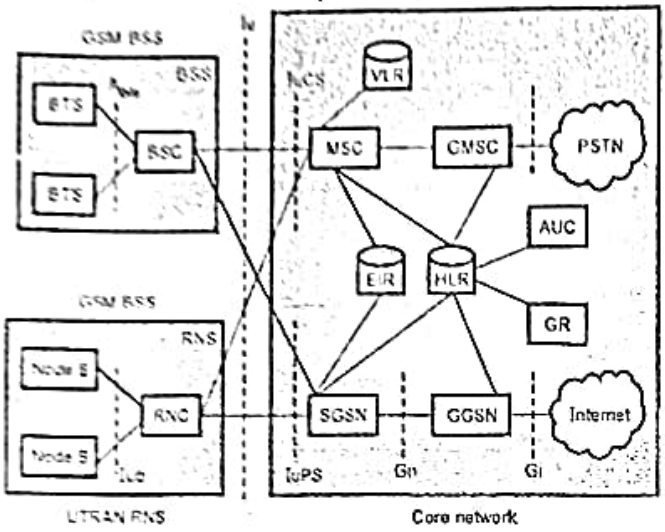
- Node B is connected to one / more antennas which creates one / more cells.
- The cell may use either FDD or TDD or both. The main function of Node B is **inner loop power control** to moderate the near far effects.
- Connection qualities and signal strengths are measured by Node B, to exercise the power control
- Node B can support **soft handover** which occurs between different antennas of the same node B.
- Node B logically equivalent to the GSM base station.
- The functions of Node B are as follows :
  1. It supports inner and open loop power control
  2. It is used for the frequency and time synchronization.
  3. It terminates U_u interface from user equipment.
  4. Radio channel coding/decoding.
  5. Error detection on transport channels.
  6. Radio channel coding/decoding.
  7. Multiplexing / demultiplexing of transport channels.

2.17.3 User Equipment (UE) :

- As shown in Fig. 2.17.2, UE is the counterpart of several nodes of architecture.
- As the counterpart of a node B, UE performs following functions :
  1. Signal quality measurements.
  2. Inner loop power control.
  3. Rate matching.
  4. Spreading and modulation.
- A the counterpart of RNC, UE performs following functions :
  1. Cooperation during handover.
  2. Cell selection.
  3. Encryption / decryption.
  4. Participation in the radio resource allocation process.
- As the counterpart of core network, UE performs following functions :
  1. It implements mobility management function.
  2. Bearer negotiation.
  3. Requests certain services from the network.

2.17.4 Core Network of UMTS (UMTS Network Architecture) :

- UMTS release 99 core network is as shown in Fig. 2.17.3 which consists of UTRAN RNS and GSM BSS. UMTS core network is similar in the context of GSM and GPRS explained earlier.

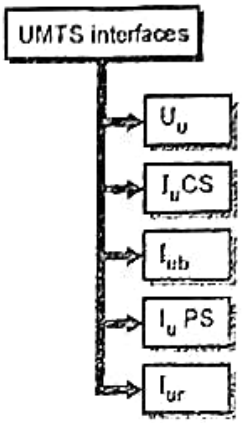


(G-2455) **Fig. 2.17.3 : UMTS core network**

- The core network is divided into two domains, circuit switched and packet switched domains.
- Some of circuit switched elements are MSC (Mobile Services Switching Centre), VLR (Visitor Location Register) and Gateway MSC (GMSC).
- Packet switched elements are SGSN (Serving GPRS Support Node) and GGSN (GPRS support node).
- Some network elements like EIR, HLR, VLR and AUC (authentication centre) are shared by both domains.
- The **Circuit Switched Domain (CSD)** is connected to RNS through IuCS interface which is a part of the Iu interface.
- The **PSD (Packet Switched Domain)** is connected to RNS through **IuPS** interface which is the part of Iu interface.
- For equipment identification both domains requires EIR database and HLR is required for location management.
- For user specific GPRS data GR (GPRS register) and for authentication AUC are included.

2.17.5 UMTS Interfaces :

- The classification of UMTS interfaces are as shown in Fig. 2.17.4.



(G-2551) **Fig. 2.17.4 : Categories of UMTS interfaces**

1. U_u : It is interface between user equipment and the network. This interface is equivalent to U_m interface in GSM/GPRS.
2. I_u-**CS** : It is circuit switched interface between UTRAN and the core voice network. It carries voice traffic and signalling between UTRAN and the core voice network. This interface is similar to A - interface in GSM/GPRS.
3. I_{ub} : RNC used this interface in order to control multiple node B's. This interface is similar to A-bis interface in GSM/GPRS. This is open and main standardized interface.
4. I_u-**PS** : This is packet switched interface between UTRAN and core data network. It carries data traffic and signalling between UTRAN and core data network. This interface is equivalent to G_b interface in GSM.
5. I_{ur} : This interface provides support to inter MSC mobility. Mobile subscriber's data is transferred to new RNC when mobile subscriber is moving between areas served by different RNCS through the I_{ur} interface. The original RNC is a **Serving RNC** is and the new RNC is a **drift RNC**. In GSM / GPRS, there is no equivalent interface.

2.17.6 UMTS Specifications / UMTS Air Interface Specifications :

Table 2.17.1 : UMTS Specifications / UMTS Air Interface Specifications

Specification	Value
Channel Bandwidth	5 MHz
Multiple access scheme	CDMA
Data Rate	384 kbps to 2 Mbps
Duplex Mode	FDD and TDD
Downlink RF Channel Structure	Direct Spread (DS)
Chip Rate	3.84 Mcps
Frame Length	10 mS
Spreading Modulation	Balanced QPSK (downlink), Dual-channel QPSK (uplink) Complex spreading circuit
Data Modulation	QPSK (downlink), BPSK (uplink)
Coherent detection	User dedicated time multiplexed pilot (downlink and uplink) Common pilot in downlink
Channel Multiplexing in Downlink	Data and control channel are multiplexed
Channel Multiplexing in Uplink	Control and pilot channel time multiplexed I & Q multiplexing for data and control channel
Multirate	Variable spreading and multicode
Spreading Factors	4-256 (uplink), 4-512 (downlink)
Frequency spectrum	Uplink 1920 MHz-1980 MHz, downlink 2110 MHz-2170 MHz.
Coding technique	Orthogonal variable spreading factor (OVSF)

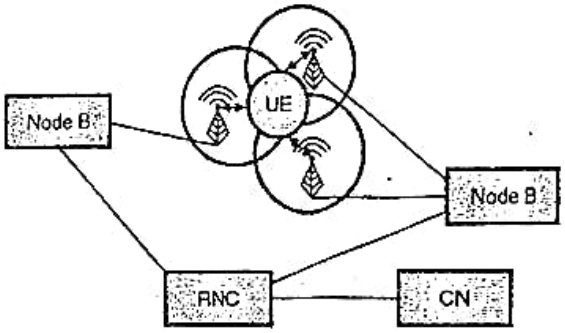
2.18 Handover / Handoff in UMTS :

Classes of handover :

1. Soft handover
2. Hard handover

2.18.1 Soft handover :

- Soft handover mechanism is available in FDD mode.
- Basic property of CDMA is **microdiversity**, due to this soft handovers are well known from traditional CDMA.
- UE may receive signals from different antennas (upto three) which belongs to several different node Bs as shown in Fig. 2.18.1(a).



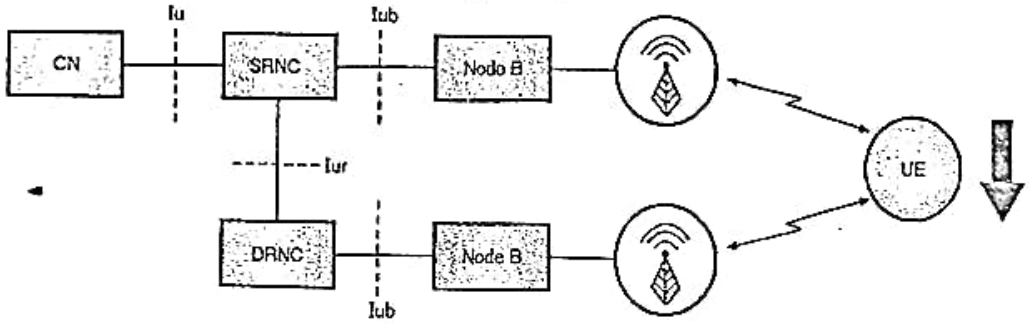
(G-2468) **Fig. 2.18.1(a) : Soft handover**

- RNC splits the data stream towards UE and it forwards it to Node Bs. Received data is again combined by UE.
- On the other direction UE sends data which is then received by all involved node Bs.
- The data streams received from the node Bs are then combined by RNC.
- At the same time UE receives data from different antennas, this fact makes handover soft.
- This is not an abrupt process as movement from one cell to another is smooth.
- With respect to shading, fading and multi-path propagation macro-diversity makes more robust transmission.
- Suppose one path is blocked by any barrier there may be good chances of receiving data using another antenna.

- At the time of soft handover, from all involved node Bs UE receives power control commands.
- As UE receives a command to lower UE lowers the transmission power which avoids interference.
- All methods related to soft handover are located in UTRAN, however it is not supported by core network.

2.18.2 Hard Handover :

- This handover is already discussed in GSM. At a certain point in time switching between different antennas / systems is performed.
- Hard handover can be used only in UTRA TDD.
- Among the slots of different frames switching between TDD cell is performed.
- Changing the carrier frequency i.e. **Inter frequency handover** is hard handover.
- At the same time receiving data at different frequencies requires more complex receiver as compared to the data receiving from different sources at the same carrier frequency.
- In UMTS all **inter system handovers** are hard handover which includes handover occurs to and from GSM or other IMT-2000 systems.
- **Inter segment handover** is special type of handover to satellite system which is again hard handover because different frequencies are used.
- UMTS defines **compressed mode** transmission of UTRA-FDD to enable UE to listen into GSM or other frequency bands. UE stops all transmission.
- Before and after the break in transmission spreading factor can be lowered or using different coding schemes less data is sent which avoids data loss.
- The situation where soft handover takes place between two node BS which do not belong to the same RNC is as shown in Fig. 2.18.1(b).

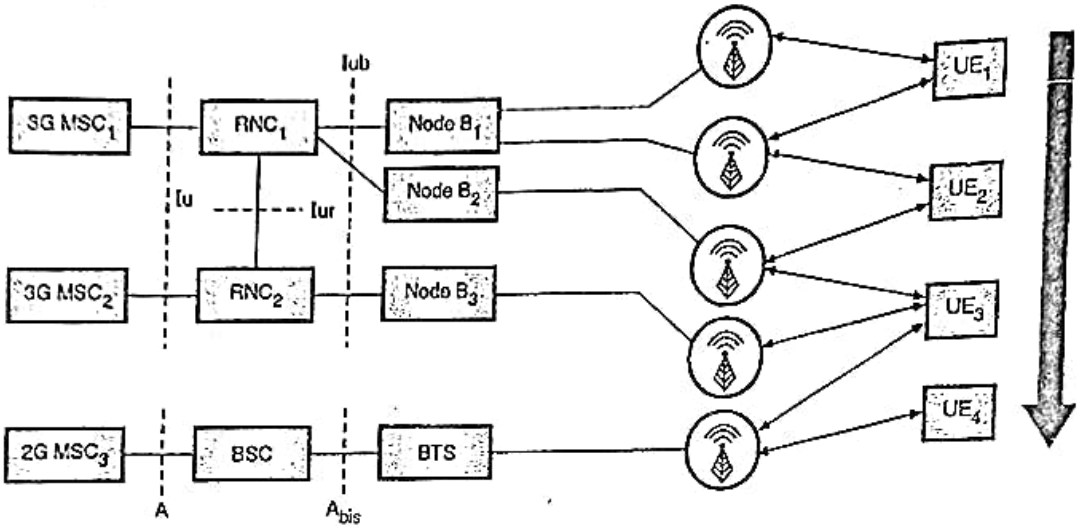


(G-2469) **Fig. 2.18.1(b) : SRNC and DRNC**

- In this case one RNC performs the connection control and it forwards all data to and from the core network.
- If the UE moves from upper to lower cell the upper RNC acts as **SRNC (Serving RNC)** whereas lower RNC acts as **DRNC (Drift RNC).**
- Via Iur interface SRNC forwards received data from the CN to its node B and to the DRNC.
- This mechanism is not available in GSM. DRNC forwards data received by the lower node B to the SRNC.
- Both data streams are combined in SRNC and single stream of data is forwarded to the CN.
- From simultaneous reception CN does not notice anything.
- If the UE moves more down and it drop out the transmission area of upper node B, resources are reserved for data transmission by two RNCS.
- SRNC relocation performed to avoid wasting resources.
- CN is involved in this process so it is hard handover.

2.18.3 Types of Handover in UMTS :

- Many common handover types in a combined UMTS / GSM network are as follows :
  1. Intra-node B, Intra-RNC
  2. Inter-node B, Intra-RNC
  3. Inter RNC
  4. Inter MSC
  5. Inter-system
- Fig. 2.18.1(c) shows overview of different handover types.



(G-2470) **Fig. 2.18.1(c) : Overview of different handover types**

1. Intra-node B, Intra-RNC :

- UE_1 goes from one antenna of node B_1, to another antenna such type of handover is known as **softer handover.**
- In this type Node B_1 performs splitting and combining of data streams.

2. Inter-node B Intra-RNC :

- From Node B_1, to node B_2, UE_2 moves. In this type by combining and splitting data RNC_1 supports the soft handover.

3. Inter-RNC :

- Two different handovers can takes place when UE_3 moves from node B_2 to B_3.
- As shown in Fig. 2.18.1(b) internal Inter-RNC handover is not visible for CN.
- In this case RNC_1 acts as SRNC and RNC_2 acts as DRNC. All the time through the interface Iu, CN will communicate.
- When relocation of Iu takes place the handover is known as **external inter-RNC handover.**
- By the same MSC_1 communication is handled now the external handover is hard handover.

4. Inter-MSC :

- It might be the case that MSC_2 takes over and it performs hard handover of the connection.

5. Inter-system :

- From a 3G UMTS network to 2G GSM network UE_4 moves on.
- For real life usability of the system this hard handover is important due to the restricted 3G coverage in the beginning.

2.19 UMTS Security Process :

Principle :

- In order to achieve the authentication features, **UMTS Authentication and Key Agreement (AKA)** security mechanism is used.
- AKA is based on challenge/response authentication protocol.
- The mobile subscriber uses AKA mechanism to verify the identity of another mobile subscriber.
- It verifies the identity without revealing a secret password shared by two parties.
- Each MS should prove to the other MS that it knows the password without revealing or transmitting the same.

- In order to complete the security process, the related information about MS should be transferred from home network to the serving network of Mobile subscriber.
- The HLR/AuC of home network provides the VLR/SGSN of serving network with authentication vectors (AVs), each one holding the information fields. AKA procedure is summarized in the following steps :

Step 1 : Requests of Authentication Vectors (AVs) :

- Visited network's VLR or SGSN requests a set of Authentication Vectors (AVs) from the HLR/AuC from the MS's home network.

Step 2 : Calculation of Authentication Vectors (AVs) :

- HLR/ AuC computes an array of AVs by means of authentication algorithm and the MS's private secret key.
- This key is stored in HLR/AuC of home network and the user Identity module (USIM) in MS's mobile subscriber.

Step 3 : Transmission of Authentication Vectors (AVs) :

- HLR /AuC responds to the visited network's VLR/SGSN by sending back n authentication vectors.

Step 4 : Challenge to MS :

- Visited network's VLR/SGSN selects a single AV and challenges the MS's USIM by sending the RAND and AUTN fields in the Authentication vector to it.

Step 5 : Verification of AVs & Generation of RES :

- The USIM of MS processes the AUTN.
- The MS with the help of private secret key K is able to verify that the received challenge data could only have been constructed by someone who had access to the same secret key.
- By checking the sequence number (SEQ) field, USIM verifies that the AV has not been expired.
- If the AV is still valid and network is authenticated, the USIM generate a confidentiality Key (CK), Integrity key (IK) and response for the network (RES).

Step 6 : Reply by MS via RES :

- The MS responds with RES to the visited network.

Step 7 : Verification of RES :

- VLR/SGSN of Visited network verifies that the response is correct.
- It verifies the response by comparing with the Expected Response (XRES) from the current AV with the response received from the USIM of mobile subscriber.

2.19.1 Advantages of UMTS :

1. Broad offer of services.
2. Speed, variety and user friendliness of a service is improved as compared with GSM.
3. Only bearer services are standardized.
4. High speed data transmission.
5. Improved voice quality.
6. Global roaming across networks.
7. Improved security.
8. Service flexibility.

2.19.2 Disadvantages of UMTS :

1. Expensive input fees for 3G service licenses.
2. It is a challenge to build the necessary infrastructure for 3G.
3. Additional expense of 3G phones.
4. Large cell phones.

2.19.3 UMTS Applications :

1. Fast Internet / intranet.
2. Streaming / download (video, audio).
3. Videoconferences.
4. Multimedia-messaging, E-mail.
5. Mobile E-commerce.
6. Location based services.
7. Mobile entertainments.

2.19.4 Comparison of UMTS and GSM :

- Table 2.19.1 gives the comparison between UMTS and GSM.

Table 2.19.1 : Comparison of UMTS and GSM

Sr. No.	Parameter	UMTS	GSM
1.	Carrier spacing	5 kHz	200 kHz
2.	Power control frequency	1.5 kHz	2 Hz or lower
3.	Quality control	Radio resource management	Network planning
4.	Packet data	Load based packet scheduling	Time slot based scheduling with GPRS
5.	Downlink transmit diversity	Supported for improving dL capacity	Not supported by standard but can be applied.

Review Questions

Q. 1 What is mobile communication ?

Q. 2 State various wireless communication systems.

Q. 3 Define the following :

1. Base station
2. Control channel
3. Forward channel
4. Reverse channel
5. Mobile station.

Q. 4 Explain the concept of half duplex communication.

Q. 5 What is a simplex communication ? Give one example.

Q. 6 Explain the concept of full duplex communication.

Q. 7 Explain FDD and TDD.

Q. 8 Explain the concept of cellular telephone system.

Q. 9 Draw general block diagram of mobile phone system and explain its operation.

Q. 10 What is MTSO ?

Q. 11 Define cell and cluster.

Q. 12 State the frequencies used in cellular telephony.

Q. 13 What is frequency reuse ?

Q. 14 Draw general block diagram of mobile phone system and explain its operation.

Q. 15 Draw block diagram of mobile phone system and explain the operation of each block.

Q. 16 Name the conditions which are controlled by the MTSO in the transreceiver.

Q. 17 What are cells ?

Q. 18 Explain the handoff procedure.

Q. 19 State the frequency bands used for mobile telephony.

Q. 20 Write a note on frequency reuse in cellular system.

Q. 21 State various handoff strategies.

Q. 22 Define "Dwell time".

Q. 23 Define :

1. Hard handoff
2. Soft hand-off

Q. 24 Explain the concept of delayed hand off and state its advantages.

Q. 25 Explain :

1. Forced handoff.
2. Queued handoff.

Q. 26 What is GSM ?

Q. 27 What are the services provided by GSM ?