1...

Basics of PCS and GSM

Chapter Outcomes...

- Describe function of the given component in PCS/GSM architecture.
- Classify the given GSM logical channel.
- Describe the given step of call processing in GSM.
- Explain the significance of given type of area in cellular network.

Learning Objectives...

- To understand Basic Concept of Wireless and Mobile Networks
- To learn Basic Concepts of PCS and GSM
- To study Typical PCS and GSM Network Architecture
- To learn Handoff and Roaming
- To understand Concept of Mobility Management and Network Signaling

1.0 INTRODUCTION

- Wireless and mobile communication networks have tremendous success in today's communication market both in general or professional usage.
- Wireless refers to a communications, monitoring or control system in which electromagnetic waves carry a signal through atmospheric space rather than along a wire.
- The evolution of radio and mobile core network technologies over the last two decades has enabled the development of the ubiquitous Personal Communication Services (PCS).
- A PCS can provide the mobile user with voice, data and multimedia services at any time, any place and in any format. The ultimate goal is to provide a PCS, which will move information of all kinds to and from people in all locations, through an advanced wireless network supporting a wide range of services.
- GSM stands for Global System for Mobile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.
- GSM Communication is a wireless communication system that uses digital cellular radio, communication to provide voice, data and multimedia applications communication services. It covers wide area of range of mobility.
- A GSM system co-ordinates the communication between mobile telephone units (mobile stations), base stations system (cell cites) and switching systems (MSC or MTSO).
- The bandwidth of each GSM radio channel is 200 KHz wide and which are further divided in to frames that hold and rime slots. GSM was originally named as Groupes Speciate Mobile.
- The Personal Communication Service (PCS) is a high frequency, low power, standards-based, wireless mobile communication system. It mainly operates within the range of 1800 to 1900 MHz.

- The principle technology base for the PCS comes from wireless analog cellular, the emerging and almost well-established digital wireless cellular systems. It has also evolved from the Global Systems for Mobile Communications (GSM) networks.
- The implementation of the PCS is based on the interconnection of various functional components that are operating in accordance with developed standards so that interoperability and reliability of the systems can be achieved.
- Personal Communications Services (PCS) is a new generation of wireless-phone technology that introduces a range of features and services surpassing those available in analog- and digital-cellular phone systems.

1.1 PERSONAL COMMUNICATION SERVICES (PCS)

- The objective of PCS is to enable communication with a person at any time, at any place and in any form. It also manages their individual call services according to their service by providing unlimited reachability and accessibility.
- The key factors of PCS are given below:
  1. Reachability with respect to Location (Home, office, in public, in transit).
  2. Accessibility with respect to Device (Cellular phone, wired phone, fax etc.).
  3. Management of Service.
- Personal communications services (PCS) refers to a wide variety of wireless access and personal mobility services provided through a small terminal, with the goal of enabling communications at any time, at any place and in any form.

Features of PCS:

- The salient features that enable PCS to provide communications with anyone, anywhere, anytime include
  1. **Roaming Ability:** The roaming service should be greatly expanded to provide universal accessibility.
  2. **Diverse Environment:** Users must be able to use the PCS in all types of environment. For example, urban, rural, commercial, residential, mountains and recreational areas.
  3. **Various Cell Size:** With PCS, there will be a mix of broad types of cell sizes. The picocell for low power indoor applications, the microcell for lower-power outdoor pedestrian application. The macrocell for high power vehicular applications and super macrocell with satellites.
  4. **Portable Handset:** PCS provides a low power radio, switched access connection to the Public Switched Telephone Network (PSTN). The user should be able to carry the handset outside without having to recharge its battery.
  5. **FCC Frequency Allocation:** The FCC frequency allocation for PCS usage is significant.FCC allocated 120 MHz for licensed operation and another 20 MHz for unlicensed operation, amounting to a total of 140 MHz for PCS, which is three times the spectrum currently allocated for cellular networks.

Advantages of PCS:

- PCS offers a number of advantages over traditional cellular communications:
  1. A truly personal service, combining lightweight phones with advanced features such as paging and voice mail that can be tailored to each individual customer.
  2. Less background noise and fewer dropped calls.
  3. An affordable fully integrated voice and text messaging that works just about anywhere, anytime.
  4. A more secure all digital network that minimizes chances of eavesdropping or number cloning.
  5. An advanced radio network that uses smaller cell sites.

1.1.1 PCS Architecture

Personal Communications Services (PCS) refers to a wide variety of wireless access and personal mobility services provided through a small terminal, with the goal of enabling communications at any time, at any place and in any form.

- Business opportunities for such services are tremendous since every person (not just every home) could be equipped as long as the service is fairly inexpensive.
- Meet of them are connected to the public switched telephone network(PSTN) to provide access to land line telephones.
- PCS technologies have grown rapidly in the telecommunications industry. Two of the most popular are High-Tier Cellular telephony, Cordless and low-Tier PCS telephony.
- These technologies have similar architectures, as shown in Fig. 1.1.

PSTN

VLR—VLR D

GMSC

HLR

MSC—BSC—MS—BTS—MSC

VLR

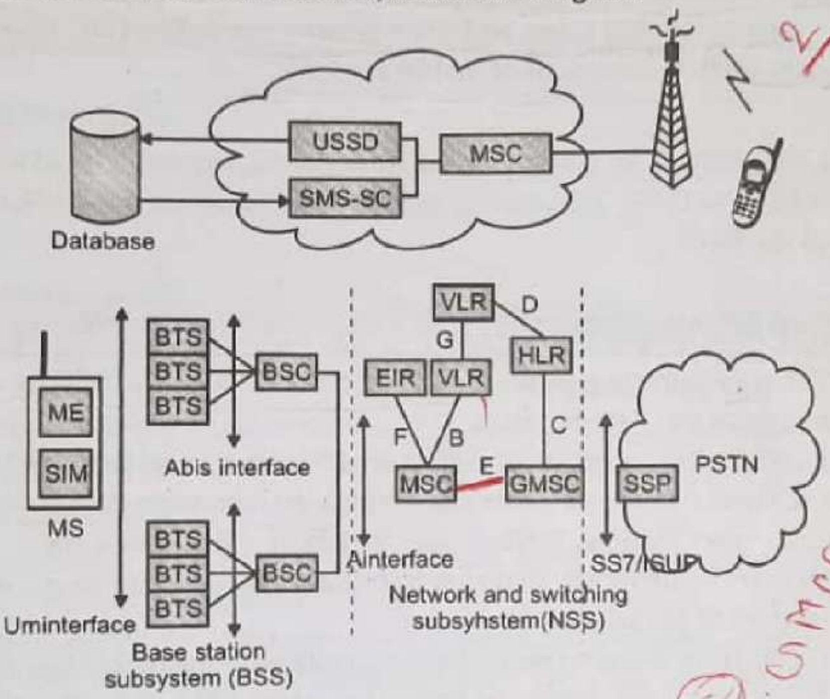


Fig. 1.1 : PCS Architecture

- Basic architecture consists of two parts:
  1. Radio Network,
  2. Wireline Transport Network

1. **Radio Network:**

- PCS use Mobile Stations (MSs) to communicate with the Base Stations (BSs) in a PCS network. MS is also referred to as handset, mobile phone, subscriber unit or portable unit.
- Modern MS technology allows the air interface to be updated (eg from DECT to GSM) over the air remotely. The MS can also be remotely monitored by the system maintenance and diagnostic capabilities.
- Different types of MSs have various power ranges and radio coverage. Hand-held MSs have a lower output power (where the maximum output power can be as low as 0.8 watts for GSM 900) and shorter range compared with vehicle-installed MSs with roof-mounted antennas (where the maximum output power can be as high as 8 watts in GSM 900)
- The radio coverage of a base station or a sector in the base station is called a cell.For systems such as GSM,CDMA and PACS the base station system is partitioned in to a controller (base station controller in GSM and radio port control unit in PACS) and radio transmitters/receivers (base transceiver stations in GSM and radio ports in PACS)

Example:

Subscriber unit: Wireless local loop.

Portable: low-tier systems (PACS).

Mobile Station: GSM system.

2. **Wireline Transport Network:**

- The base stations usually reach the wireline transport network (core or backbone network) via land links or dedicated microwave links.
- The Mobile Switching Center(MSC) connected to the base station is a special switch tailored to mobile applications.
- The Ericsson MSC is based on its AXE switching platform. The MSC is connected to the PSTN to provide services between the PCS users and the wire-line users. The MSC also communicates with mobility databases to track the locations of mobile stations.

Example:

The Lucent 5ESS MSC 2000 is an MSC modified from Lucent Technologies 5ESS switching system. The Siemens D900/1800/1900 GSM switch platform is based on its EWSD (Digital Electronic Switching System) platform.

1.2 GSM NETWORK ARCHITECTURE

GSM stands for Global System for Mobile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.

- The GSM network architecture consists of different elements that all interact together to for... the overall GSM system. These include elements like the base-station, controller, MSC, AuC, HLR, VLR, etc.
- The GSM technical specifications define the different elements within the GSM network architecture. It defines the different elements and the ways in which they interact to enable the overall system operation to be maintained.
- *The GSM network architecture is now well established and with the other later cellular systems now established and other new ones being deployed, the basic GSM network architecture has been updated to interface to the network elements required by these systems.*
- *Despite the developments of the newer systems, the basic GSM system architecture has been maintained, and the network elements described below perform the same functions as they did when the original GSM system was launched in the early 1990s. GSM network architecture element.*
- *The GSM network architecture as defined in the GSM specifications can be grouped into four main areas:*
  1. *Mobile Station (MS).*
  2. *Base-Station Subsystem (BSS).*
  3. *Network and Switching Subsystem (NSS).*
  4. *Operation and Support Subsystem (OSS).*
- *The different elements of the GSM network operate together and the user is not aware of the different entities within the system.*
- ***A basic diagram of the overall GSM system architecture with these four major elements is shown** below:*

1. ***Mobile Station:***

- *Mobile Stations (MS), Mobile Equipment (ME) or as they are most widely known, cell or mobile phones are the section of a GSM cellular network that the user sees and operates.*

- In recent years their size has fallen dramatically while the level of functionality has greatly increased. A further advantage is that the time between charges has significantly increased.
- A further advantage is that the time between charges has significantly increased. There are a number of elements to the cell phone, although the two main elements are the main hardware and the SIM.
- The hardware itself contains the main elements of the mobile phone including the display, case, battery, and the electronics used to generate the signal, and process the data receiver and to be transmitted. It also contains a number known as the International Mobile Equipment Identity (IMEI).
- This is installed in the phone at manufacture and "cannot" be changed. It is accessed by the network during registration to check whether the equipment has been reported as stolen.
- The SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network. It contains are variety of information including a number known as the International Mobile Subscriber Identity (IMSI).

2. Base Station Subsystem (BSS):

- The Base Station Subsystem (BSS) section of the GSM network architecture that is fundamentally associated with communicating with the mobiles on the network.
- It consists of two elements:

(i) Base Transceiver Station (BTS):

- The BTS used in a GSM network comprises the radio transmitter receivers, and their associated antennas that transmit and receive to directly communicate with the mobiles.
- The BTS is the defining element for each cell. The BTS communicates with the mobiles and the interface between the two is known as the Um interface with its associated protocols.

(ii) Base Station Controller (BSC):

- The BSC forms the next stage back into the GSM network. It controls a group of BTSs, and is often co-located with one of the BTSs in its group.
- It manages the radio resources and controls items such as handover within the group of BTSs, allocates channels and the like. It communicates with the BTSs over what is termed the Abis interface.

3. Network Switching Subsystem (NSS):

- The GSM system architecture contains a variety of different elements, and is often termed the core network.
- It provides the main control and interfacing for the whole mobile network. The major elements within the core network include:

(i) Mobile Services Switching Centre (MSC):

- The main element within the core network area of the overall GSM network architecture is the Mobile switching Services Centre (MSC). The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality to enable the requirements of a mobile user to be supported.
- These include registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber.
- It also provides an interface to the PSTN so that calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to be made to mobiles on different networks.

(ii) Home Location Register (HLR):

- This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS.
- When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position.
- There is one HLR per network, although it may be distributed across various sub-centers to for operational reasons.

(iii) Visitor Location Register (VLR):

- This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided.
- The VLR can be implemented as a separate entity, but it is commonly realised as an integral part of the MSC, rather than a separate entity. In this way access is made faster and more convenient.

(iv) Gateway Mobile Switching Centre (GMSC):

- The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location.
- The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC.
- The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.

(v) SMS Gateway (SMS-G):

- The SMS-G or SMS gateway is the term that is used to collectively describe the two Short Message Services Gateways defined in the GSM standards. The two gateways handle messages directed in different directions.
- The SMS-GMSC (Short Message Service Gateway Mobile Switching Centre) is for short messages being sent to an ME. The SMS-IWMSC (Short Message Service Inter-Working Mobile Switching Centre) is used for short messages originated with a mobile on that network.
- The SMS-GMSC role is similar to that of the GMSC, whereas the SMS-IWMSC provides a fixed access point to the Short Message Service Centre.

(vi) IWF: Using Additional Interworking Function, MSC can also connect to public data network.

4. Operation and Support Subsystem (OSS):

- • The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC.
- It is used to control and monitor the overall GSM network and it is also used to control the traffic load of the BSS.
- It must be noted that as the number of BS increases with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing savings in the cost of ownership of the system.

(i) Equipment Identity Register (EIR):

- The EIR is the entity that decides whether given mobile equipment may be allowed onto the network.

- Each mobile equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration.
- Dependent upon the information held in the EIR, the mobile may be allocated one of three states - allowed onto the network, barred access, or monitored in case its problems.

(ii) Authentication Centre (AuC):

- The AuC is a protected database that contains the secret key also contained in the user's SIM card.
- It is used for authentication and for ciphering on the radio channel.

(iii) Operational Subsystem (OMC):

- Monitors and maintains the performance of all other entities such as MS, BS, and BSC.OMC is Responsible for traffic monitoring, subscriber and security management, Accounting and Billing.

GSM Network Interfaces:

- The different interfaces used to provide communication between various elements in a GSM cell phone network The network structure is defined within the GSM standards.
- Additionally each interface between the different elements of the GSM network is also defined. This facilitates the information interchanges can take place.
- It also enables to a large degree that network elements from different manufacturers can be used. However as many of these interfaces were not fully defined until after many networks had been deployed, the level of standardization may not be quite as high as many people might like.

1. **Um Interface:** The "air" or radio interface standard that is used for exchanges between a mobile (ME) and base station (BTS / BSC). For signalling, a modified version of the ISDN LAPD, known as LAPDm is used.

A bis

2. **Abis Interface:** This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardised. The Abis interface allows control of the radio equipment and radio frequency allocation in BTS.

A — BSC

3. **A Interface:** The A interface is used to provide communication between the BSS and the MSC. Interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipments being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface.
4. **B Interface:** The B interface exists between the MSC and the VLR . It uses protocol known as the MAP/B protocol. As most VLRs are collocated with an MSC, this makes interface purely an "internal" interface. The interface is used whenever the MSC needs access to data regarding a MS located in its area.

C

5. **C Interface:** The C interface is located between the HLR and a GMSC or a SMS-G. When a call originates from outside network, i.e. from PSTN or another mobile network it ahs to pass through gateway so that routing information required to complete the call may be gained. The protocol used for communication is MAP/C, the letter "C" indicating that the protocol is used for the "C" interface. In addition to this, MSC may optionally forward billing information to the HLR after the call is completed and cleared down.

D

6. **D Interface:** The D interface is situated between the VLR and HLR. It uses MAP/D protocol to exchange data related to the location of the ME and to the management of the subscriber.
7. **E Interface:** The E interface provides communication between two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol.

MSC $\overset{E}{—}$ MSC

F

8. **F Interface:** The F interface is used between an MSC and EIR. It uses the MAP/F protocol. The communications along this interface are used to confirm status of the IMEI of the ME gaining access to the network.

A

9. **G Interface:** The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure.

10. **H Interface:** The H interface exists between the MSC the SMS-G. It transfers short messages and uses the MAP/H protocol.

H

rd

11. **I Interface:** The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through the BSS.

I

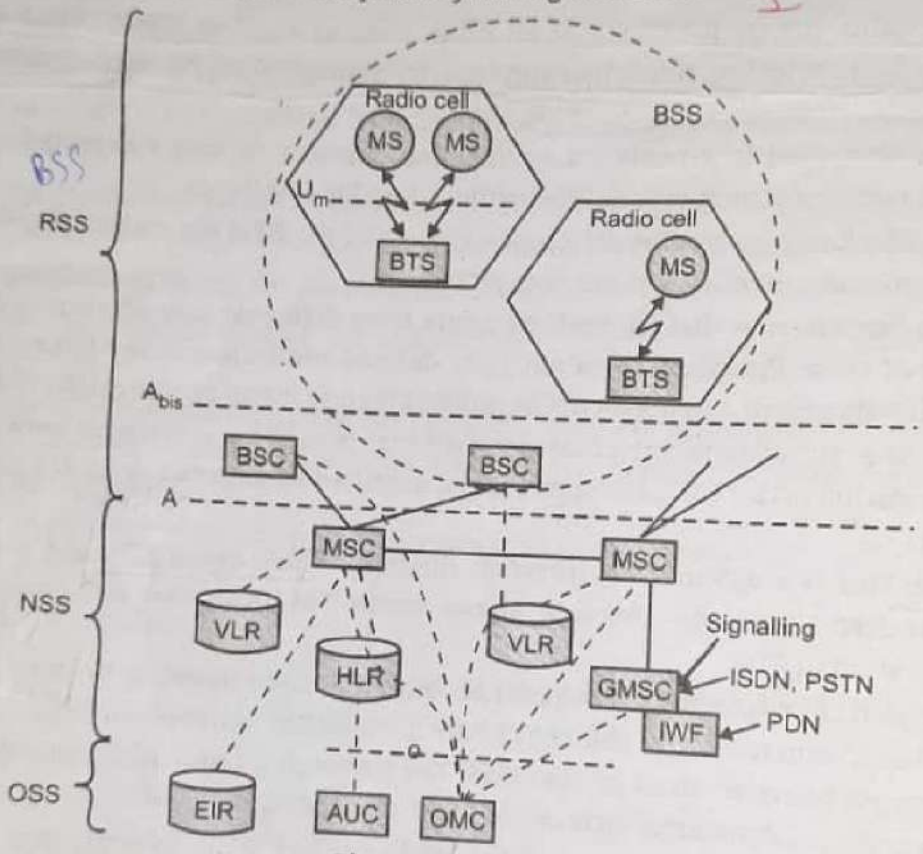


Fig. 1.2 : GSM Architecture

1.2.1 GSM Frequency Spectrum

For Cellular communication only narrow bandwidth is allocated. The frequencies and spectrum allocated for GSM is listed below:

GSM 900:

Uplink: 890 MHz to 915 MHz. — uplink GSM 900 (890-915) MHz

Downlink: 935 to 960MHz. — d.wnli GSM 900 (935-960) MHz

Absolute Radio Frequency Channels (ARFCN)-124.

EGSM 900:

Uplink: 880 MHz to 915 MHz.

Downlink: 925 MHz to 960 MHz.

Absolute Radio Frequency Channels (ARFCN)-174.

GSM 1800(DCS 1800):

Uplink: 1710 MHz to 1795 MHz.

Downlink: 1805 MHz to 1880 MHz.

Absolute Radio Frequency Channels (ARFCN)-374.

PCS 1900:

Uplink: 1850 MHz to 1910 MHz.

Downlink: 1930 MHz to 1990 MHz.

Absolute Radio Frequency Channels (ARFCN)-299.

GSM uses TDMA & FDMA

1.2.2 Radio Aspects of GSM

- In GSM uplink (mobile to base) frequency band is 800-915 MHz, resulting in 45 MHz spacing for duplex operation.
- The GSM uses TDMA and FDMA whereby the available 25 MHz spectrum is partitioned in to 124 carriers (carrier spacing=200 KHz) and each carrier in turn is divided in to 8 time slots(radio channels).
- Each user transmits periodically in every eighth time slot in the uplink radio carrier and receives in a corresponding time slot on the down link carrier.
- The several conversations can take place simultaneously at the same pair of transmit/receive radio frequencies. The radio parameters for GSM are summarized in Table 1.1.

Table 1.1

Sr. No.	Parameter	Specification
1.	Reverse channel frequency	890-915MHZ
2.	Forward channel frequency	935-960MHZ
3.	ARFCN Number	0 to 124 and 975 to1023
4.	Tx/Rx frequency spacing	45 MHZ
5.	Tx/Rx Time slot spacing	3 Time slot
6.	Modulation data rate	270.833333kbps
7.	Frame period	4.615ms
8.	User per frame	8
9.	Time slot period	576.9microsecond
10.	Bit period	3.692microsecond
11.	Modulation	0.3GMSK
12.	ARFCN channel spacing	200 kHZ
13.	Interleaving	40ms
14.	Voice coder bit rate	13.4kbps

3.692 ms

1.2.3 GSM Services

- GSM provides integrated services for voice and data. There are three types of services delivered by a GSM system as, Teleservices, Bearer (or data) services and Supplementary ISDN services.
- They also include subservices. The various services offered by a GSM system are as under:

1. **Telephone Services:**

- Standard mobile telephone, Mobile-originated
- Base-originated traffic, emergency calling
- Fax, Videotext

channel
TCH
CH

2. **Tele text, SMS, MMS (Supplementary Services):**

- Supplementary ISDN services:
- Call diversion, Caller line ID
- Closed user group, Call barring
- Call waiting, Call hold
- Connected line ID

3. **Multiparty (Teleconferencing):**

- Call charge advice
- This service also include the Short Messaging Service (SMS) which allow GSM subscriber and BS to transmit alphanumeric pages of limited length (160 -7 ASCII characters) while simultaneously carrying normal voice traffic.

1.2.4 GSM Channel Types

- In GSM cellular communication, logical channels are a portion of a physical channel that is used for a particular (logical) communication purpose.
- The physical channel may be divided in time frequency or digital coding to provide for these logical channels.
- Classification of GSM logical channels and function of each channel:

1. **GSM traffic channel (TCH):**

- GSM TCH may be either full rate or half rate and may carry either digitized speech or user data.

1 **Full Rate TCH:**

- (a) **Full rate speech channel (TCH/FS):** This channel carries user speech which is digitized at a raw data rate if 13kbps. With GSM channel coding added to the digitized speech, this channel carries 22.8kbps.
- (b) **Full rate data channel for 9600 bps(TCH/F9.6):** This channel carries raw user data which is sent at 9600 bps. With additional forward error correction coding applied by GSM standard the 9600bps data is sent at 22.8kbps.
- (c) **Full Rate Data Channel for 4800bps(TCH/F4.8):** This channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by GSM standard the 4800bps data is sent at 22.8kbps.
- (d) **Full Rate Data Channel for 2400bps (TCH/F2.4):** This channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by GSM standard the 2400bps data is sent at 22.8kbps.

2 **Half Rate TCH:**

- (a) **Half Rate Speech Channel (TCH/HS):** This channel has been designed to carry digitized speech which is sampled at half rate of 6.5kbps. with GSM channel coding added to the digitized speech the half rate speech channel will carry data at 11.4kbps.
- (b) **Half Rate Data Channel for 4800bps (TCH/H4.8):** This channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by GSM, this channel will carry data at 11.4kbps.
- (c) **Half Rate Data Channel for 2400bps (TCH/H2.4) :** This channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by GSM, this channel will carry data at 11.4kbps.

18-21

5

6M

2. GSM Control Channel (CCH):

- The 184-bit packet from data link layer is formatted for the data burst bits. The 184-bits are added after 40 party bits, four bits and 224 hold convolution coding bits to result in the 456-bit packet.
- There are three main types of control channels in the GSM system. They are: (1) Broadcast channel (2) Common control channel (3)Dedicated control channel.

Broadcast Channel (BCH):

- **Broadcast Control Channel (BCCH):**The BCCH is a forward control channel that is used to broadcast information such as cell and network identity, operating characteristics of the cell (current control channel structure, channel availability and congestion). The BCCH also broadcast a list of channels that are currently in use within the cell.
- **Frequency Correction Channel (FCCH):** The FCCH allows each subscriber unit to synchronize its internal frequency standard (local oscillator) to the exact frequency of the base station.
- **Synchronization Channel (SCH):** SCH is used to identify the serving BS while allowing each mobile to frame synchronizes with the BS. The Frame Number (FN) is sent with the base station identity code (BSIC) during the SCH burst.

Common Control Channel (CCCH):

- **Paging Channel (PCH):** The PCH provides paging signals from the BS to all mobiles in the cell, and notifies a specific mobile of an incoming call which originates from PSTN. PCH may be used to provide cell broadcast ASCII text messages to all subscribers.
- **Random Access Channel (RACH):** The RACH is a reverse link channel used by a subscriber unit to acknowledge a page from the PCH and is also used by mobiles to originate a call.
- **Access Grant Channel (AGCH):** The AGCH is used by the BS to provide forward link communication to the mobile, and carries data which instructs the mobile to operate in a particular physical channel.

Dedicated Control Channel (DCCH):

- **Stand-alone Dedicated Control Channel (SDCCH):** The SDCCH carries signaling data following the connection if the mobile with the BS, and just before TCH assignment issued by the BS. The SDCCH ensures that the mobile station and base station remain connected while the BS and MSC verifies subscriber unit.
- **Slow Associated Control Channel (SACCH):** On the forward link the SACCH is used to send slow but regularly changing control information to the mobile such a transmit power level instruction. On the reverse link the SACCH carries information about the received signal strength.
- **Fast Associated Control Channel (FACCH):** FACCH carries urgent messages and contains essentially the same type of information as SDCCH.

Necessity of Logical Channel in GSM System:

- In practice, a multimode terminal used by a third generation (3G) mobile communication system network will have to scan for suitable frequency band or channel, identify application radio and standard and select from among the set or available services.
- If it develops at a very large number of frequency bands need to be scanned and the many standards need to be searched registering such a roaming multimode terminal by means of systematic

scanning procedure will become very inefficient, tending to degrade quality of service for the users perspective.

- This problem can be alleviated by using common physical or logical broadcast channel called the global radio control channel.
- Therefore, there is a necessity of logical channel in GSM system to scan a single frequency or a small range of frequency and thereby find the required information on available network or standards and services.

1.2.5 Messages and Call Processing in GSM System

In this section we study we study messages and processing in GSM system.

Messages in GSM:

- The types of messages to be transmitted over the Reverse control channel are Page response message, origination message, order confirmation message and older message.
- All messages contain an application message header, mandatory fixed parameters, mandatory variable parameters, remaining length and optical variable parameters.

Call Processing in GSM:

- The Mobile station call processing in GSM consists of the following four types:
  1. Mobile station initiation state.
  2. Mobile station idle state.
  3. System access state.
  4. Mobile station control on the traffic channel state.

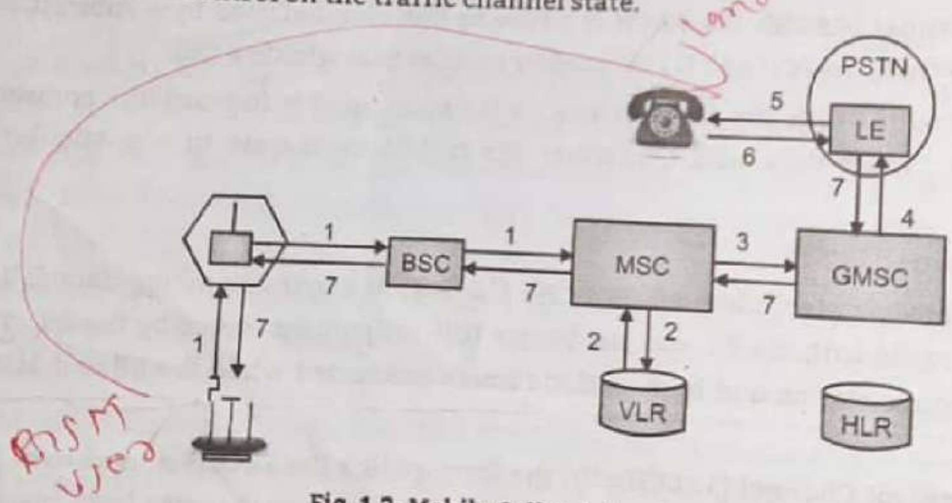


Fig. 1.3: Mobile Call Origination in GSM

Mobile Call Origination in GSM:

- The MS sends the dialed number indicating service requested to the MSC(via BSS).
- The MSC checks from the VLR if the MS is allowed the requested service. If so, MSC asks BSS to allocate necessary resources for the call.
- If the call is allowed, the MSC routes the call to GMSC.
- The GMSC routes the call to the local exchange of called user.
- The LE alerts (applies ringing) the called terminal.
- Answer back (ring back tone) from the called terminal to LE.
- Answer back signal is routed back to the MS through the serving MSC which also completes the speech path to the MS.

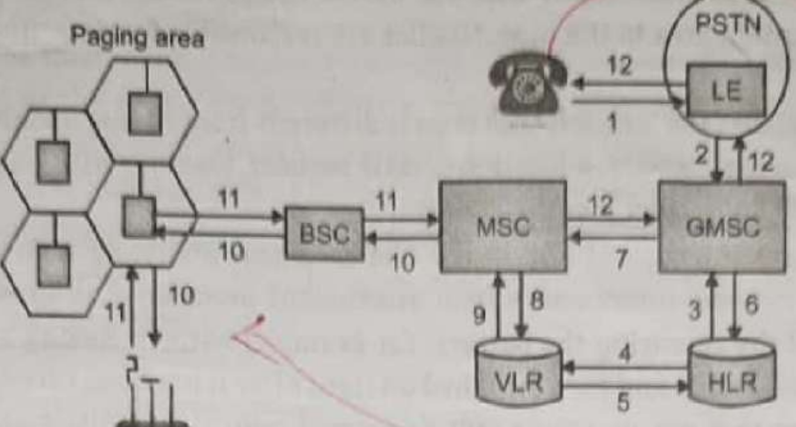


Fig. 1.4 : Mobile Call termination in GSM

Mobile Call Termination:

- The PSTN user dials the MSISDN of the called user in GSM.
- The LE routes the call to the GMSC of the called GSM user.
- The GMSC uses the dialed MSISDN to determine the serving HLR for the GSM user and interrogates it to obtain the required routing number.
- The HLR requests the current serving VLR for the called MS for a MSRN (MS roaming number) so that the call can be routed to the correct MSC.
- The VLR passes the MSRN to the HLR.
- The HLR passes the MSRN to the GMSC.
- Using the MSRN, the GMSC routes the call to the serving MSC.
- The MSC interrogates the VLR for the current Location Area Identity (LAI) for the MS.
- The VLR provides the current location for the MS.
- The MSC pages MS via the appropriate BSS. The MS responds to the page and sets up the necessary signaling links.
- When the BSS has established the necessary radio links, the MSC is informed an the call is delivered to the MS. When the MS answers the call, the connection is completed to the calling PSTN user.

1.3 MOBILITY MANAGEMENT

- Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work.
- The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

1.3.1 Location Update Procedure

- A GSM or UMTS network, like all cellular networks, is basically a radio network of individual cells, known as base stations. Each base station covers a small geographical area which is part of a uniquely identified location area.
- By integrating the coverage of each of these base stations, a cellular network provides a radio coverage over a much wider area. For GSM, a base station is called a Base Transceiver Station (BTS), and for UMTS it is called a Node B. A group of base stations is named a location area, or a routing area.

- The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting Location Area Codes (LAC).
- When a mobile finds that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI).
- The mobile also stores the current LAC in the SIM card, concatenating it to a list of recently used LACs. This is done to avoid unnecessary IMSI attachment procedures in case the mobile has been forced to switch off (by removing the battery, for example) without having a chance to notify the network with an IMSI detach and then switched on right after it has been turned off.
- Considering the fact that the mobile is still associated with the Mobile Switching Center/Visitor Location Register (MSC/VLR) of the current location area, there is no need for any kind of IMSI attachment procedures to be done.
- There are several reasons why a mobile may provide updated location information to the network. Whenever a mobile is switched on or off, the network may require it to perform an IMSI attach or IMSI detach location update procedure.
- Also, each mobile is required to regularly report its location at a set time interval using a periodic location update procedure. Whenever a mobile moves from one location area to the next while not on a call, a random location update is required.
- This is also required of a stationary mobile that reselects coverage from a cell in a different location area, because of signal fade. Thus, a subscriber has reliable access to the network and may be reached with a call, while enjoying the freedom of mobility within the whole coverage area.
- When a subscriber is paged in an attempt to deliver a call or SMS and the subscriber does not reply to that page then the subscriber is marked as absent in both the MSC/VLR and the Home Location Register (HLR) (Mobile not reachable flag MNRF is set).
- The next time the mobile performs a location update, the HLR is updated and the mobile not reachable flag is cleared.

1.3.2 Temporary Mobile Subscriber Identity (TMSI)

- The Temporary Mobile Subscriber Identity (TMSI) is the identity that is most commonly sent between the mobile and the network.
- TMSI is randomly assigned by the VLR to every mobile in the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.
- The network can also change the TMSI of the mobile at any time. And it normally does so, in order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface.
- This makes it difficult to trace which mobile is which, except briefly, when the mobile is just switched on, or when the data in the mobile becomes invalid for one reason or another.
- At that point, the global International Mobile Subscriber Identity (IMSI) must be sent to the network. The IMSI is sent as rarely as possible, to avoid it being identified and tracked.
- A key use of the TMSI is in paging a mobile. "Paging" is the one-to-one communication between the mobile and the base station.
- The most important use of broadcast information is to set up channels for "paging". Every cellular system has a broadcast mechanism to distribute such information to a plurality of mobiles.
- Size of TMSI is 4 octet with full hex digits and can't be all FF because the SIM uses 4 octets with all bits equal to 1 to indicate that no valid TMSI is available.

GG

1.3.3 Roaming

- Roaming is one of the fundamental mobility management procedures of all cellular networks.
- Roaming is defined as the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network.
- This can be done by using a communication terminal or else just by using the subscriber identity in the visited network. Roaming is technically supported by a mobility management, authentication, authorization and billing procedures.

1.3.4 Types of Area:

- The different types of area in wireless and mobile network are ① Location area, ② Routing area, ③ Tracking area.

1. **Location Area:**

- A "location area" is a set of base stations that are grouped together to optimize signaling. Typically, tens or even hundreds of base stations share a single Base Station Controller (BSC) in GSM, or a Radio Network Controller (RNC) in UMTS.
- The BSC / RNC is the intelligence behind the base stations; it handles allocation of radio channels, receives measurements from the mobile phones, and controls handovers from base station to base station.
- To each location area, a unique number called a Location Area Code (LAC) is assigned. The location area code is broadcast by each base station at regular intervals.
- Within a location area, each base station is assigned a distinct Cell Identifier (CI) number, see also Cell Global Identity.
- If the location areas are very large, there will be many mobiles operating simultaneously, resulting in very high paging traffic, as every paging request has to be broadcast to every base station in the location area.
- This wastes bandwidth and power on the mobile, by requiring it to listen for broadcast messages too much of the time.
- If on the other hand, there are too many small location areas, the mobile must contact the network very often for changes of location, which will also drain the mobile's battery. A balance has therefore to be struck.

2. **Routing Area:**

- The routing area is the packet-switched domain equivalent of the location area. A "routing area" is normally a subdivision of a "Location Area". Routing areas are used by mobiles which are GPRS-attached.
- GPRS is optimized for "bursty" data communication services, such as wireless internet/intranet, and multimedia services. It is also known as GSM-IP ("Internet Protocol") because it will connect users directly to Internet Service Providers
- The bursty nature of packet traffic means that more paging messages are expected per mobile, and so it is worth knowing the location of the mobile more accurately than it would be with traditional circuit-switched traffic.
- A change from routing area to routing area (called a "Routing Area Update") is done in an almost identical way to a change from location area to location area. The main differences are that the Serving GPRS Support Node (SGSN) is the element involved.

3. **Tracking Area:**

The tracking area is the LTE counterpart of the location area and routing area. A tracking area is a set of cells. Tracking areas can be grouped into lists of tracking areas (TA lists), which can be configured on the User Equipment (UE).

- Tracking area updates are performed periodically or when the UE moves to a tracking area that is not included in its TA list.
- Operators can allocate different TA lists to different UEs. This can avoid signaling peaks in some conditions for instance, the UEs of passengers of a train may not perform tracking area updates simultaneously.
- On the network side, the involved element is the Mobility Management Entity (MME). MME configures TA lists using NAS messages like Attach Accept, TAU Accept or GUTI Reallocation Command.

1.3.5 Mobility Management (PCS)

- The performance of the PCS network is significantly affected by the way the network manages the movements of the mobile users.

PCS System Architecture:

- The mobile service area is covered by a set of base stations (BSs)., which are responsible for relaying the calls to and from the mobile stations (MSs) located in their coverage areas (or cells).
- The BSs are connected to mobile switching centers (MSCs) by land links.
- MSC is a telephone exchange configured specifically for mobile applications, interfaces the MSs (via BSs) with the PSTN.
- Database are used for roaming management : Home Location Register (HLR) and Visitor location Register (VLR).
- There are two aspects of mobility in a PCS network namely, Roaming and Handoff.

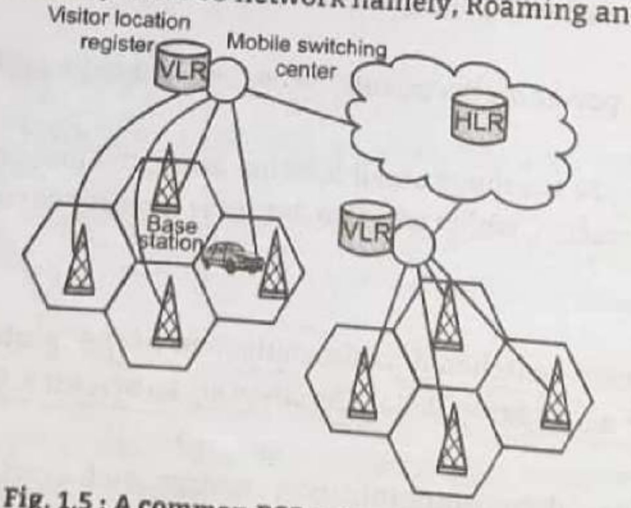


Fig. 1.5 : A common PCS network architecture

1. **Roaming:**

- When a mobile user moves from one PCS system (e.g., the system in New York City) to another (e.g. the system in Los Angeles), the system should be informed of the current location of the user. Otherwise it would be impossible to deliver the services to the mobile user.
- To support mobility management, protocols such as EIA/TIA Interim Standard 41 (IS-41 or ANSI-41) or Global System for Mobile Communications(GSM),Mobile Application Part(MAP) have been defined for PCS networks.

– MCHO NCHO MAHO } Hand-off

2. Handoff:

- When a mobile user is engaged in conversation, the MS is connected to a BS via a radio link.
- If the mobile user moves to the coverage area of another BS, the radio link to the old BS is eventually disconnected, and a radio link to the new BS should be established to continue the conversation.
- This process is variously referred to as automatic link transfer, handover or handoff. Three strategies have been proposed to detect the need for handoff namely, Mobile - Controlled Handoff (MCHO), Network-Controlled Handoff (NCHO) and Mobile-Assisted Handoff (MAHO).

1. Mobile-Controlled Handoff (MCHO):

- The MS continuously monitors the signals of the surrounding BSs and initiates the handoff process when some handoff criteria are met.
- MCHO is used in DECT and PACS.

2. Network-Controlled Handoff (NCHO):

- The surrounding BSs measure the signal from the MS, and the network initiates the handoff process when some handoff criteria are met.
- NCHO is used in CT-2 Plus and AMPS.

AMPS – First gen cellular system

3. Mobile-Assisted Handoff(MAHO):

- The network asks the MS to measure the signal from the surrounding BSs. The network makes the handoff decision based on reports from the MS.
- MAHO is used in GSM and IS-95 CDMA.

Two Types of Handoff:

1. The BSs involved in the handoff may be connected to the same MSC (inter-cell handoff or inter-BS handoff)
2. The BSs involved in the handoff may be connected to two different MCSs (intersystem handoff or inter-MSC handoff)

Inter-BS Handoff:

- The new and the old BSs are connected to the same MSC. Assume that the need for handoff is detected by the MS. The following actions are taken:
  1. The MS momentarily suspends conversation and initiates the handoff procedure by signaling on an idle (currently free) channel in the new BS. Then it resumes the conversation on the old BS.
  2. Upon receipt of the signal, the MSC transfers the encryption information to the selected idle channel of the new BS and sets up the new conversation path to the MS through that channel. The switch bridges the new path with the old path and informs the MS to transfer from the old channel to the new channel.
  3. After the MS has been transferred to the new BS, it signals the network, and resumes conversation using the new channel.
  4. Upon receipt of the handoff completion signal, the network removes the bridge from the path and releases resources associated with the old channel.
- This handoff procedure is used with the mobile-controlled handoff strategy.

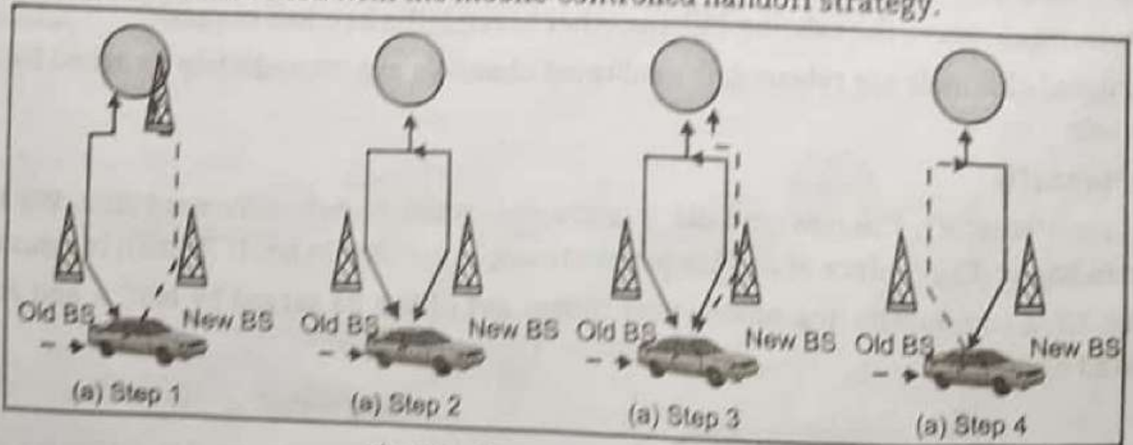


Fig. 1.6. : Inter-BS link transfer

Inter-BS Handoff:

- For the network-controlled handoff strategy all handoff signaling messages are exchanged between the MS and the old BS though the failing link.
- The whole process must be completed as quickly as possible, to ensure that the new link is established before the old link fails. If the new BS does not have an idle channel. The handoff call may be dropped(or forced to terminate)
- The forced termination probability is an important criterion in the performance evaluation of a PCS network. Forced termination of an ongoing call is considered less desirable than blocking a new call attempt.
- Most PCS networks handle a handoff in the same manner as a new call attempt. That is if no channel is available, the handoff is blocked and the call is held on the current channel in the old cell until the call is completed or when the failing link is no longer available.
- This is referred to as the non-prioritized scheme. These handoff schemes can significantly reduce the probability of forced termination as well as the probability of call incompletion (new call blocking plus handoff call forced termination).

Channel Assignment Schemes:

- To reduce forced termination and to promote call completion, three channel assignment schemes have been proposed, Reserved channel scheme, Queuing priority scheme, subrating scheme.

1. **Reserved Channel Scheme:**

- Similar to the non-prioritized scheme, except that some channels in each BS are reserved for handoff calls.

2. **Queuing Priority Scheme:**

- Adjacent coverage areas of BSs may overlapped.
- Thus, there is considerable area where a call can be handled by either BS. This area is called the handoff area.
- If no channel is available in the new BS during handoff, the new BS buffers the handoff request in a waiting queue.
- The MS continues to use the channel with the old BS until either a channel in the new BS becomes available (and the handoff call is connected) or the MS moves out of the handoff area(and the call is forced to terminate)

3. **Subrating Scheme:**

- Creates a new channel for a handoff call by sharing resources with an existing call if no channel is available in the new BS.
- Subrating means an occupied full rate channel is temporarily divided in to two channels at half the original rate: one to serve the existing call, the other to serve the handoff request.
- When occupied channels are released, the subrated channels are immediately switched back to full rate channels.

Intersystem Handoff:

- In intersystem handoff, the new and old BSs are connected to two different MSCs. We trace the intersystem handoff procedure of IS-41 ,where network-controlled handoff (NCHO) is assumed.
- In this Fig. 1.7, a communicating mobile user moves out of the BS served by MSC A and enters the area covered by MSC B.

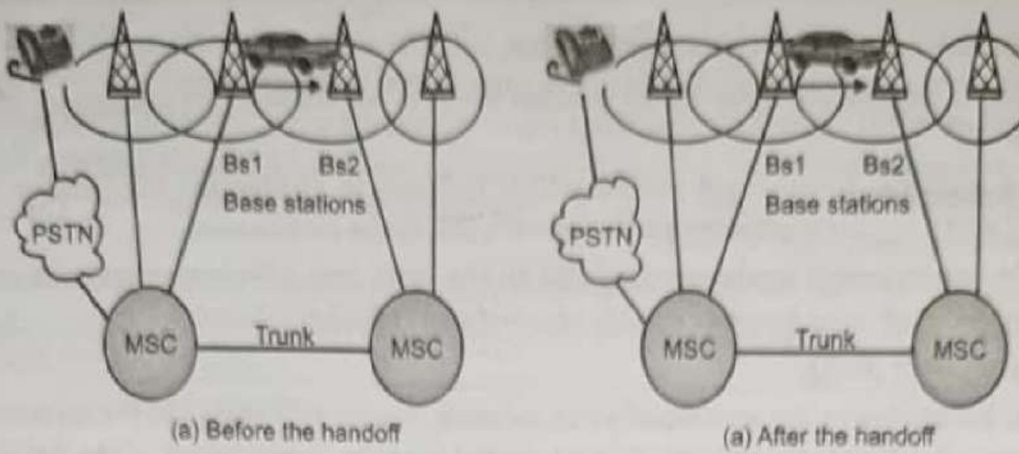


Fig. 1.7 : Intersystem handoff

Intersystem Handoff Requires the Following Steps:

Step 1: MSC A requests MSC B to perform handoff measurements on the call in progress. MSC B then selects a candidate BS2,BS2 and interrogates it for signal quality parameters on the call in progress. MSC B returns the signal quality parameter values, along with other relevant information, to MSC A.

Step 2: MSC A checks if the MS has made too many handoffs recently. (this is to avoid, for example numerous handoffs between BS1 and BS2 a where the MS is moving within the overlapped area) or if intersystem trunks are not available. If so, MSC A exits the procedure. Otherwise, MSC A asks MSC B to set up a voice channel. Assuming that a voice channel is available in BS2,MSC B instructs MSC A to start the radio link transfer.

Step 3: MSC A sends the MS a handoff order. The MS synchronizes to BS2.After the MS is connected to BS2, MSC B informs MSC A that the handoff is successful. MSC A then connects the call path(trunk) to MSC B and completes the handoff procedure.

- In this intersystem handoff process, MSC A is referred to as the anchor MSC, and is always in the call path before and after the handoff, as illustrated in the four cases in Fig. 1.8.
- This anchor approach is used in all existing mobile phone networks because the re-establishment of a new call path(without involving MSC A) between MS and the new MSC would require extra trunk release/setup operations in PSTN, which is not available or is not cost-effective.
- If the MS moves back to MSC A again, the connection between MSC A and MSC B is removed (handoff backward). If the MS moves to the third MSC C ,then MSC B will be in the call path(handoff to third).
- Note that when the MS moves to the third MSC, the second MSC may be removed from the call path. That is, the link between MSC B and MSC A is disconnected and MSC C connects to MSC A directly. This process is called path minimization.

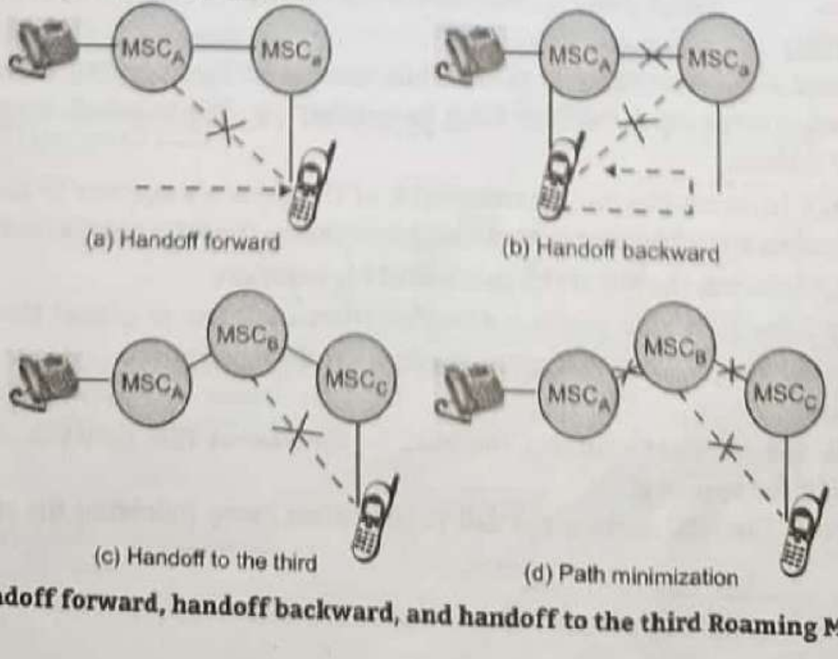


Fig. 1.8 : Handoff forward, handoff backward, and handoff to the third Roaming Management:

- Two basic operations in roaming management are
  1. Registration (or location update), the process whereby an MS informs the system of its current location
  2. Location tracking, the process during which the system locates the MS.Location tracking is required when the network attempts to deliver a call to the mobile user.
- The roaming management strategies proposed in the IS-41 and GSM MAP standards are two-level strategies in that they use a two-tier system of home and visited databases.

Home Location Register (HLR):

- When a user subscribes to the services of a PCS network, a record is created in the systems' database, called the home location register(HLR). This is referred to as the home system of the mobile user.
- The HLR is a network database that stores and manages all mobile subscriptions of a specific operator.
- Specifically, the HLR is the location register to which an MS identity is assigned for record purposes, such as directory number, profile information, current location and validation period.

Visitor Location Register (VLR):

- When the mobile user visits a PCS network other than the home system, a temporary record for the mobile user is created in the visitor location register(VLR) of the visited system.
- The VLR temporarily stores subscription information for the visiting subscribers so that the corresponding MSC can provide service.
- In other words, the VLR is the "other" location register used to retrieve information for handling calls to or from a visiting mobile user.

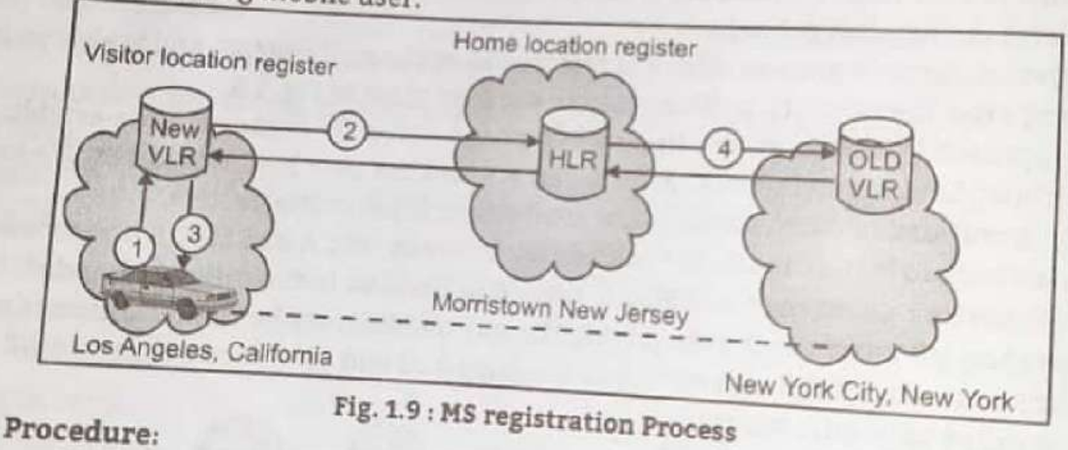


Fig. 1.9 : MS registration Process

Registration Procedure:

Step 1: Suppose that the home system of a mobile user is in Morristown. When the mobile user moves from one visited system (eg. New York City) to another (eg. Los Angeles), it must register in the VLR of the new visited system.

Step 2: The new VLR informs the mobile users HLR of the person's current location-the address of the new VLR. The HLR sends an acknowledgement ,which includes the MS's profile, to the new VLR.

Step 3: The new VLR informs the MS of the successful registration.

Step 4: After step 2,the HLR also sends a deregistration message to cancel the obsolete location record of the MS in the old VLR. The old VLR acknowledges the deregistration.

Call Delivery Procedure:

- To originate a call, the MS first contacts the MSC in the visited PCS network. The call request is forwarded to the VLR for approval.
- If the call is accepted, the MSC sets up the call to the called party following the standard PSTN call setup procedure.

Step 1: If a wireline phone attempts to call a mobile subscriber, the call is forwarded to a switch, called the originating switch in the PSTN, which queries the HLR to find the current VLR of the MS(1). The HLR queries the VLR in which the MS resides to get a routable address(2). If the originating switch is not capable of querying the HLR(i.e. it is not equipped to support mobility),the call is routed through the PSTN to the subscribers gateway MSC, which queries the HLR to determine the current VLR serving the MS.

Step 2: The VLR returns the routable address to the originating switch through the HLR.

Step 3: Based on the routable address, a trunk (voice circuit) is set up from the originating switch to the MS through the visited MSC.

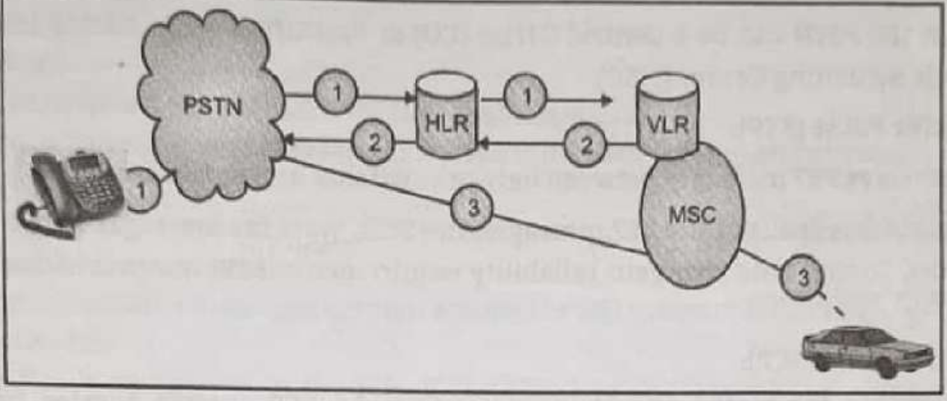


Fig. 1.10 : Call delivery procedure

Roaming Management Under SS7:

- The missing parts in the picture are the interactions between the PCS network and the PSTN.
- This section briefly describes how mobile roaming is managed by the PSTN signaling.

Common Channel Signaling(CCS):

- Common channel signaling (CCS) is a signaling method that provides control and management functions in the telephone network. CCS consists of supervisory functions, addressing and call information provisioning.
- A CCS channel conveys messages to initiate and terminate calls, determine the status of some part of the network and controls the amount of traffic allowed. CCS uses a separate out-of-band signaling network to carry signaling messages.

SS7:

- Signaling System No 7(SS7) is a CCS system developed to satisfy the telephone operating companies requirements for an improvement to the earlier signaling systems, which lacked the sophistication required to deliver much more than Plain Old Telephone Service (POTS).
- Signaling between a PCS network and the PSTN are typically achieved by the SS7 network. In this network, the trunks (voice circuits) connect SSPs to carry user data/voice information.
- The signaling links connect SCPs to STPs, and STPs to SSPs. The SSPs and SCPs are connected indirectly through STPs.

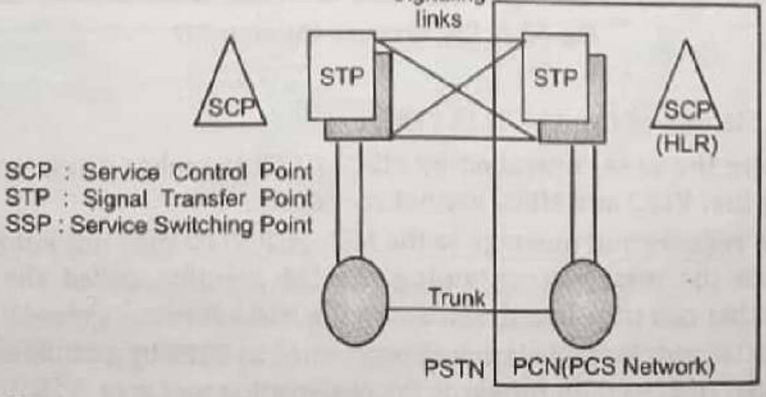

Signaling links
STP
STP
SCP
SCP
(HLR)
SCP : Service Control Point
STP : Signal Transfer Point
SSP : Service Switching Point
Trunk
PSTN
PCN(PCS Network)

Fig. 1.11 : Interconnection between a PCS network and the PSTN

- Fig. 1.11 shows the network elements that are involved in the interconnection between a PCS network and the PSTN. In the fig the dashed lines represent the signaling links, the solid lines represent a trunk.
- The SS7 network consists of three distinct components namely, Service Switching Point (SSP), Signal Transfer Point (STP) and Service Control Point (SCP).

1. **Service Switching Point(SSP):**

- A telephone switch interconnected by SS7 links. The SSPs perform call processing on calls that originate, tandem, or terminate at that node.
- A local SSP in the PSTN can be a Central Office (CO) or End Office (EO). An SSP in a PCS network is called a Mobile Switching Center (MSC).

2. **Signal Transfer Point (STP):**

- A switch that relays SS7 messages between network switches and databases.
- Based on the address fields of the SS7 messages, the STPs route the messages to the correct outgoing signaling links. To meet the stringent reliability requirements, STPs are provisioned in mated pairs as shown in Fig.

3. **Service Control Point(SCP):**

- Contains databases for providing enhanced services. An SCP accepts queries from an SSP and returns the requested information to the SSP. In mobile applications, an SCP may contain an HLR or a VLR.

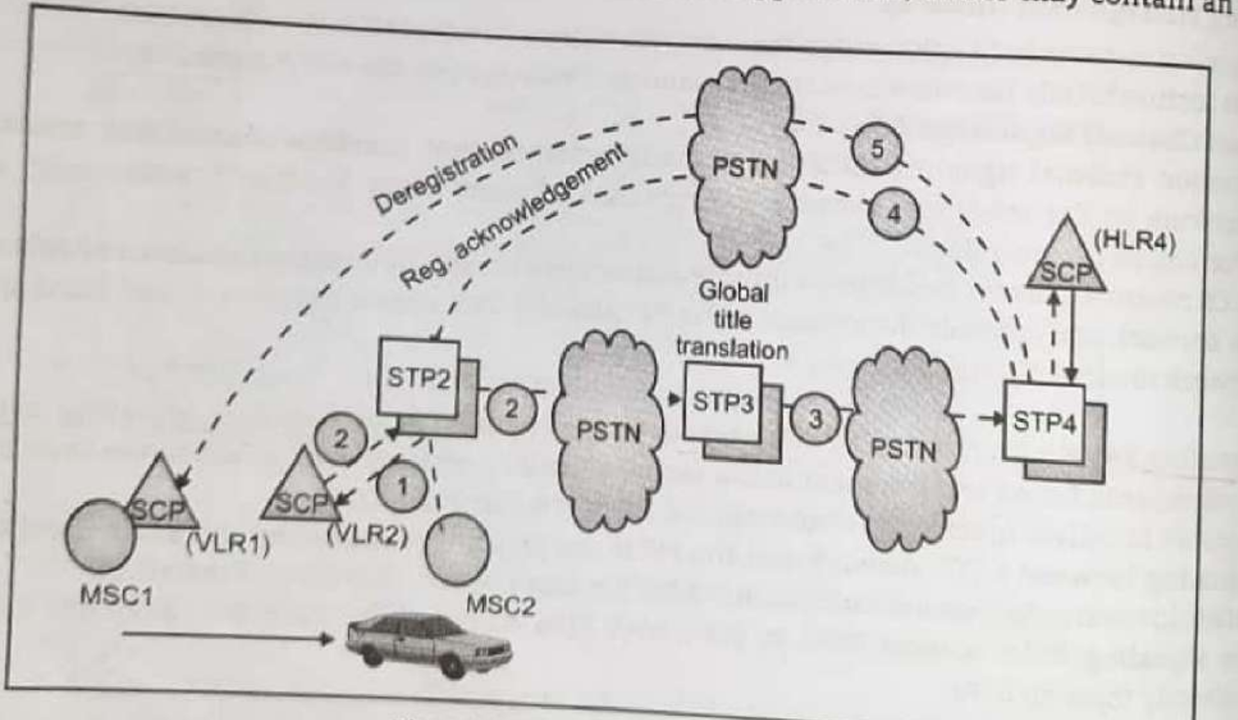


Fig. 1.12 : Registration through SS7

Registration:

- In this example, the MS moves from VLR1 to VLR2

Step 1: The MS enters the area controlled by MSC2.MSC2 launches a registration query to its VLR through STP2,assuming that VLR2 and MSC2 are not co-located.

Step 2: VLR2 sends a registration message to the MS's HLR.VLR2 may not know the actual address of HLR. Instead,VLR2 sends the message containing the MS identity, called the Mobile Identification Number(MIN),to an STP that can translate the MIN into the HLR address.

Step 3: The MIN-to-HLR address translation is performed at STP3 by a table-lookup technique called Global Title Translation(GTT). STP3 then forwards the registration message to HLR.

Step 4: After the registration, HLR sends an acknowledgement back to VLR2. Since the address of VLR2 is known, the acknowledgement may be sent to VLR2 using a shortcut, without passing through STP3.

Step 5: After step3,HLR sends a deregistration message to VLR1 to cancel the obsolete record.VLR1 then acknowledges the cancellation.

- In steps 2, 3, 4 and 5, the messages may visit several STPs before arriving at their destinations, and the registration process may generate considerable traffic in the SS7 network.
- Thus it is desirable to reduce the registration traffic.
- Two approaches have been proposed to reduce the "cost" of deregistration at step 5. Implicit deregistration, periodic re-registration.

Implicit Deregistration:

- Obsolete VLR records are not deleted until the database is full.
- If the database is full when an MS arrives, a record is deleted, freeing storage space to accommodate the newly arrived MS.
- A replacement policy is required to select a record for replacement (it is possible that a valid record is replaced, and the information is lost).

Advantage: No deregistration messages are sent among the SS7 network elements.

Periodic re-registration:

- The MS periodically reregisters to the VLR. If the VLR does not receive the re-registration message within a timeout period, the record is deleted.
- This approach only creates local message traffic between the MSC and the VLR. Furthermore no SS7 signaling messages are generated if the VLR is co-located with the MSC.

Pointer Forwarding Scheme:

- To reduce the registration traffic at steps 2 and 3 in Fig. 1.13, a pointer forwarding scheme was proposed which consists of two operations: Move operation (registration), Find operation (call delivery).

Move Operation (Registration):

- When an MS moves from one VLR to another, a pointer is created from the old VLR to the new VLR.
- No registration to the HLR is required.

Find Operation (Call Delivery):

- When the HLR attempts to locate the MS for call delivery, the pointer chain is traced. After the find operation, the HLR points directly to the destination VL.

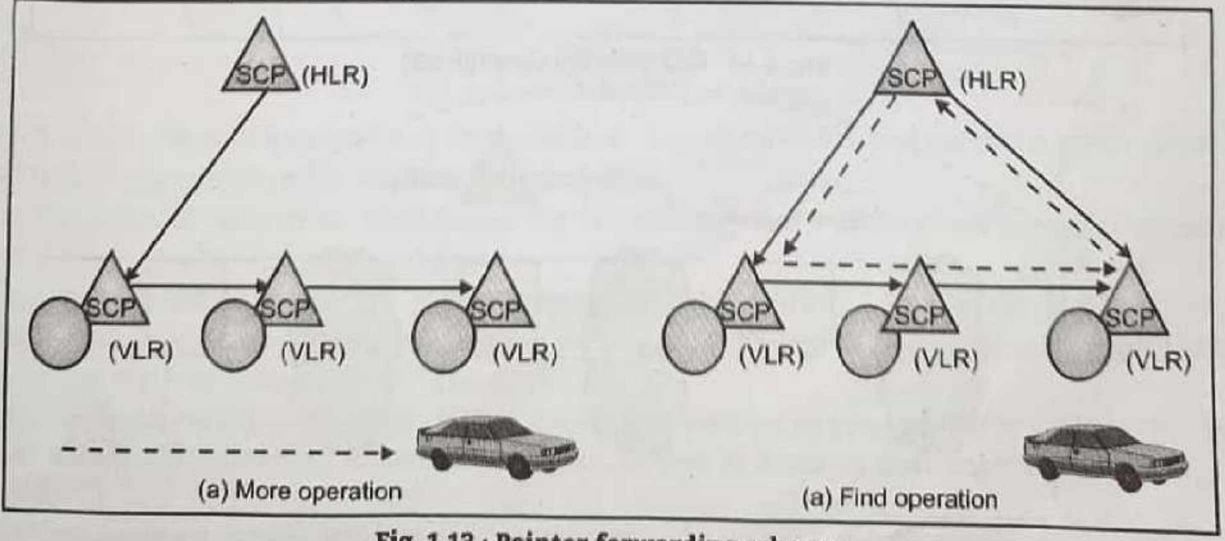


Fig. 1.13 : Pointer forwarding scheme

- Depending on the memory capacities of the VLRs, the pointers in the obsolete chain may not be deleted. To limit the pointer traversal time in the find operation, the registration procedure in Fig. 1.12 may be performed for every k move operations.

- In other words, the number of pointers visited in the find operation will be limited by k. The pointer forwarding scheme should not be considered when the net cost of pointer creation and pointer traversal is higher than the cost of accessing the HLR.
- As performance studies indicate, the pointer forwarding scheme significantly reduces the network traffic in many cases.

Call Delivery:

- Similar to the registration process, visits to several STPs and a GTT may be required to access the HLR in call delivery. Several STPs may be visited to obtain the routable address from the VLR.
- To reduce the call delivery traffic, a cache scheme was proposed to maintain a cache in the originating SSPs. Another possibility is to maintain the cache in the STP that performs GTTs that is STP3 in Fig. 1.13.
- A cache entry consists of two fields: the MIN of an MS and the address of the current visited VLR of the MS. The cache contains entries for MSs recently accessed from the SSP.

Cache Scheme:

- When the calling party originates a call to an MS, the SSP first checks if the cache entry for the MS exists. There are three possibilities:

  Case 1: The cache entry does not exist. The call delivery procedure illustrated in Fig. 1.15.

  Case 2: The cache entry exists and is current. The VLR is directly accessed as shown in Fig. 1.15.

  Case 3: The cache entry exists but is obsolete. The procedure detects that the cache entry is obsolete if the queried VLR's response is negative. The call delivery procedure is illustrated in Fig. 1.15.

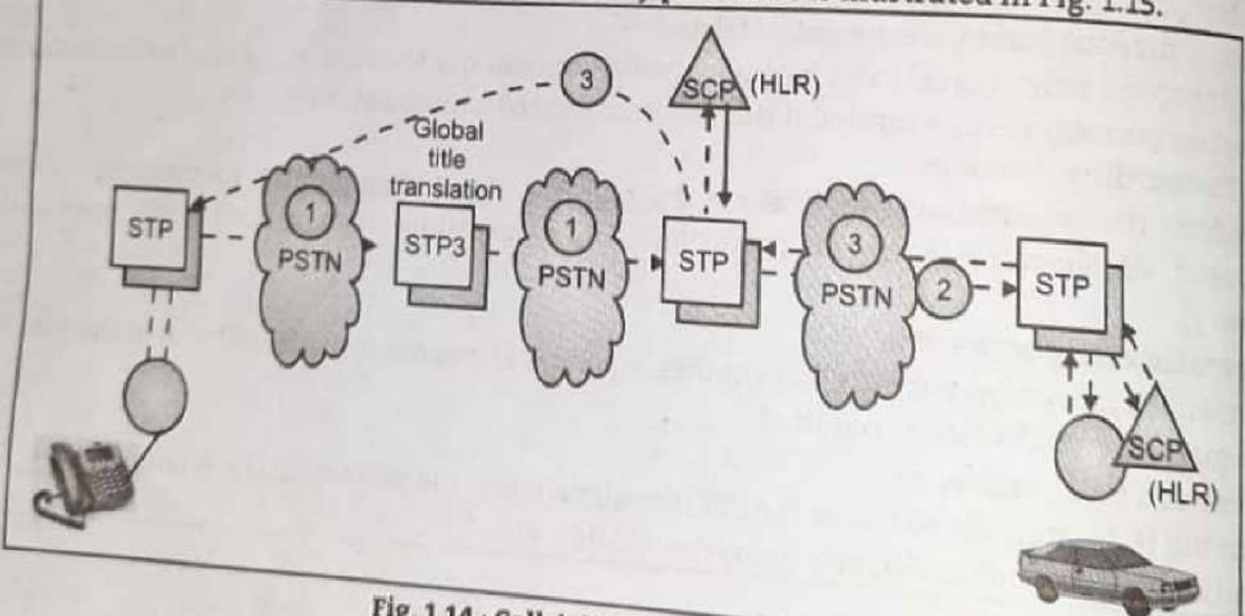
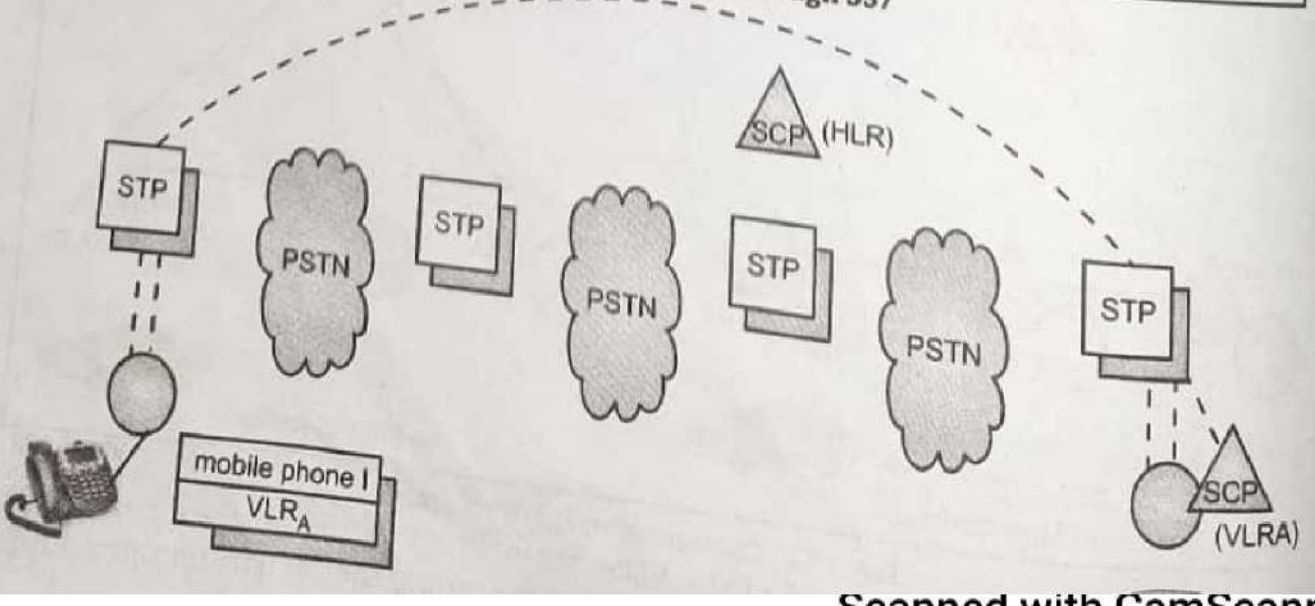


Fig. 1.14 : Call delivery through SS7



Discussion:

- Note that implicit deregistration and periodic re-registration can be used with the cache scheme, but the obsolete cache information may not be detected until the MS is paged.
- Since the cache information may be obsolete, some heuristics are required to determine whether the cached information will be used to locate the MS.
- One technique is to have the SSP estimate the cache hit ratio, or the probability that case 2 is true. If the probability is high, the entry is considered "current" and is enabled; otherwise the entry is disabled.
- Another heuristic determines the obsoleteness of an entry based on the period that an MS resides in a VLR as indicated in the cache entry.
- If the cache entry indicates that the MS has stayed in a VLR for a period longer than a specified threshold, the entry is assumed to be obsolete.
- The threshold can be adjusted in real time based on cache hit statistics. If case 3 is more likely to occur than case 2, then the cache scheme should not be considered.
- Performance studies indicate that the cache scheme significantly seduces the call delivery cost in many case.

Roaming Management for CT-2:

- In a public environment,CT2 is a one-way calling PCS system; that is a CT2 handset can originate outgoing calls, but cannot receive incoming calls.
- We describe how to construct two-way calling mechanism in to CT2.As we will demonstrate later, introducing roaming management for CT2 is expensive.
- Nevertheless, this introduction provides a model so that the reader can understand the design complexity required to implement a total mobility solution for an one-way PCS system.

Basic Public CT2 System (One-WAY calling):

- Fig. 1.16 shows basic public CT2 system.

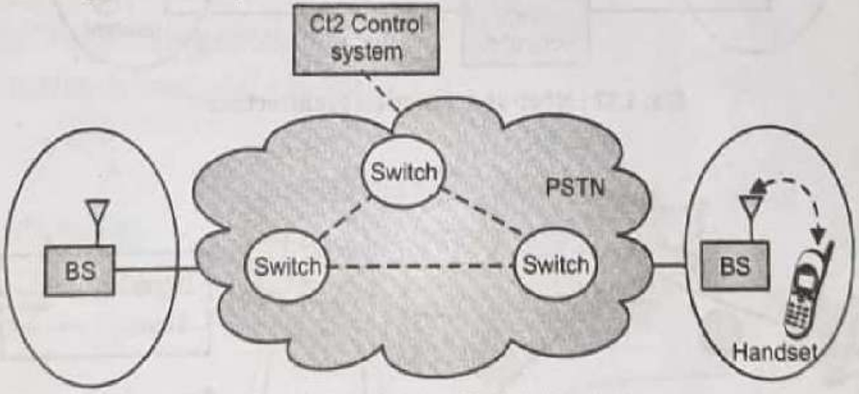


Fig. 1.16 : Basic Public CT2 System

- The original public CT2 system was designed as a tele-point service, and did not support call delivery. CT2 BS is connected directly to a switch in the PSTN.
- The CT2 control system is responsible for monitoring and building, which may be connected indirectly to the BSs through the PSTN.
- The messages between the CT2 control system and the BSs are delivered through the PSTN. CT2 system csn provide only the call origination service. It is impossible to provide call delivery service as in cellular systems such as DAMPS and GSM.
- Some CT2 systems (eg. the systems in Hong Kong) utilized the paging system to provide call delivery; thus when a wireline user A wanted to call a CT2 user B, A would first page B through the paging system.
- From the paging message, B identified the telephone number of A, then dialed back to A through the CT2 system.

Advantage:

1. No modifications are made to the CT2 architecture.

Disadvantages:

1. The inconvenience caused by the involvement of the paging system and thus for the reverse charging.
2. Also if both A and B use CT2 handsets in different CT2 systems it is impossible to connect the call.

Meet-at-a-Junction CT2 System (Two-Way Calling):

- An advanced CT2 system may follow the "meet-at-a-junction" approach to provide the call delivery capability.
- The CT2 architecture for this approach is illustrated in Fig. 1.16.
- In this approach, the CT2 service area is partitioned in to several location areas.
- All BSs in the same location area are connected to an area controller.
- Through the Public Switched Data Network (PSDN) all area controllers are connected to the database, called the location register.

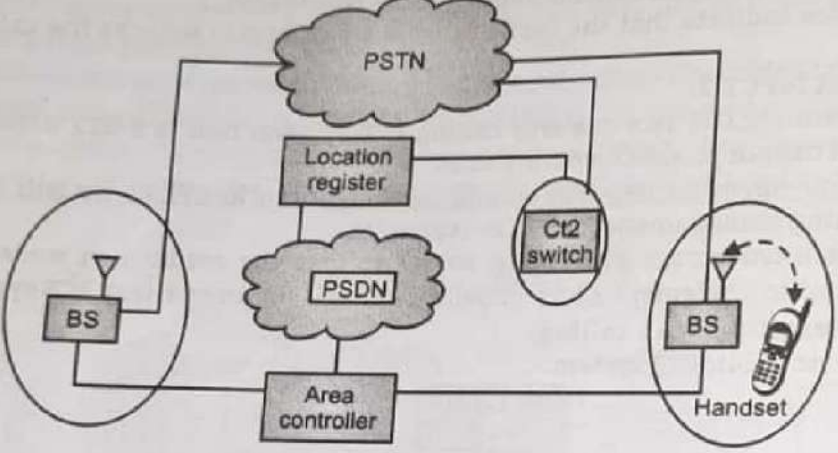


Fig. 1.17 : Meet-at-a-junction architecture

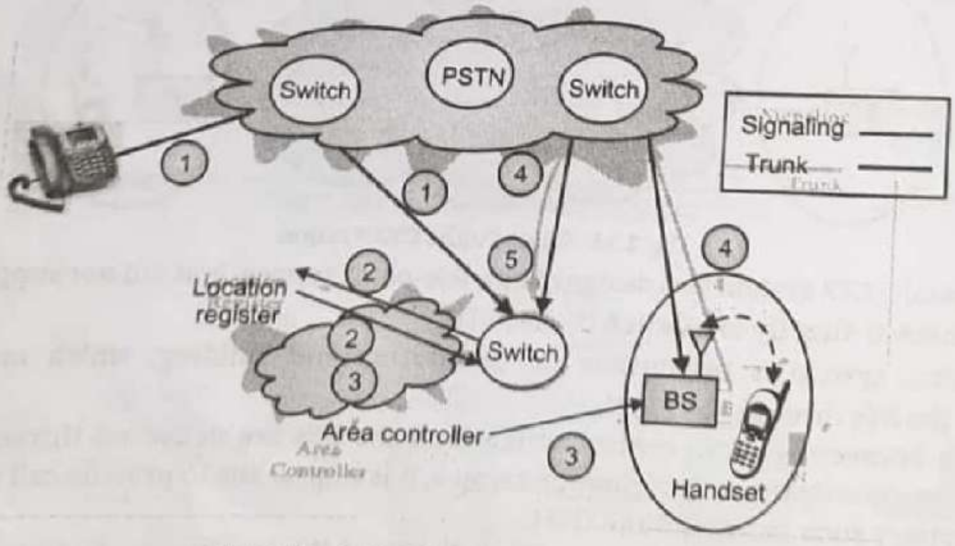


Fig. 1.18 : CT2 call delivery procedure

Call Delivery Procedure:

- A handset will register at the location register after it enters a location area. A location record for the handset is created in the location register, which indicates the location area-the address of the corresponding area controller, where the handset resides.

- From the registration list of the location register, the BSs poll the handsets periodically. If the polled handset does not reply, the CT2 system assumes that the handset has left the location area and the handset's location is deleted.
- If a handset does not receive the polling message for a long time, for example when the handset moves to a new location area and the movement is not known by the location register, the handset registers to reclaim its existence.
- The call delivery procedure is described in the following steps:

  Step 1: When the calling party dials the number of a CT2 handset, a voice trunk is set up from the originating switch to the CT2 switch S1.

  Step 2: S1 queries the location register to identify the area controller of the handset.

  Step 3: An alerting message is sent from S1 to the corresponding area controller via the PSDN. The area controller then broadcasts the alerting message to the connected BSs to page the handset.

  Step 4: If the handset responds, the corresponding base station redials to S1 through the PSTN.

  Step 5: S1 bridges the two trunks, and the conversation begins.
- Two dials are required in the call delivery procedure: One from the originating switch to S1 and the other from the BS to S1.
- The CT2 modifications for two-way calling services have been considered expensive. In Taiwan, for example, a CT2 call delivery was considered as two phone calls.
- The CT2 services in Hong Kong were terminated in 1996.In the same year, many European countries replaced CT2 by DECT as the standard cordless technology. In Taiwan, the bandwidth for CT2 was reclaimed for PACS and PHS in 2000.

1.3.6 GSM Mobility Management

- Fig. 1.17 shows mobility management in GSM.

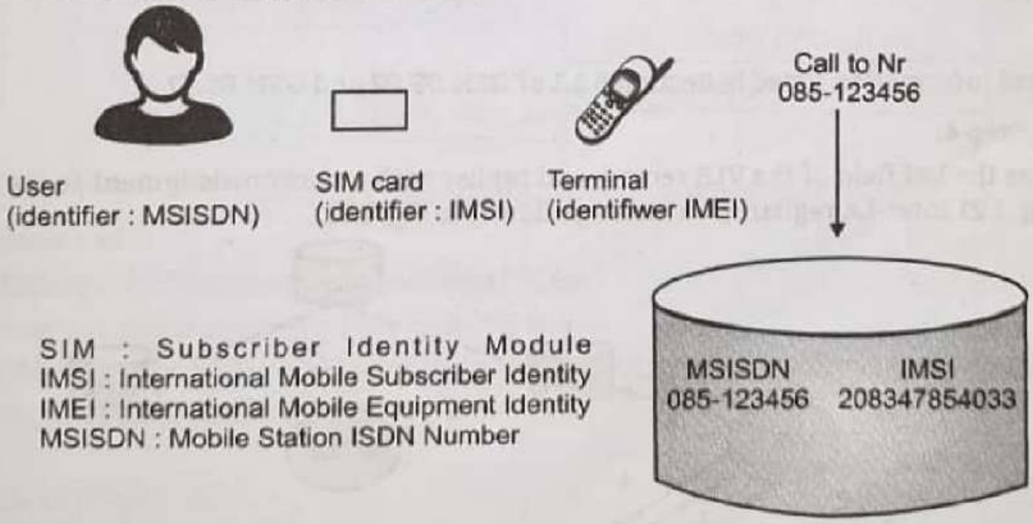

Call to Nr
085-123456
User
(identifier : MSISDN)
SIM card
(identifier : IMSI)
Terminal
(identifiwer IMEI)
SIM : Subscriber Identity Module
IMSI : International Mobile Subscriber Identity
IMEI : International Mobile Equipment Identity
MSISDN : Mobile Station ISDN Number
MSISDN
IMSI
085-123456
208347854033

Fig. 1.19 : GSM Mobility Management

- GSM networks track the locations of the MSs so that incoming calls can be delivered to subscribers. A mobile service area is partitioned into several Location Area (LAs) or registration areas LA consists of a group of Base Transceiver Stations (BTSs) that communicate with the MSs over radio links.

GSM Location Area Hierarchy:

- In GSM, registration or location update occurs when an MS moves from one LA to another.
- Basic Location Update Procedure contains Inter-LA Movement, Inter-MSC Movement and Inter-VLR Movement. MS cannot distinguish the types of movement

Inter-LA Movement:

- Fig. 1.20 shows inter-la movement.

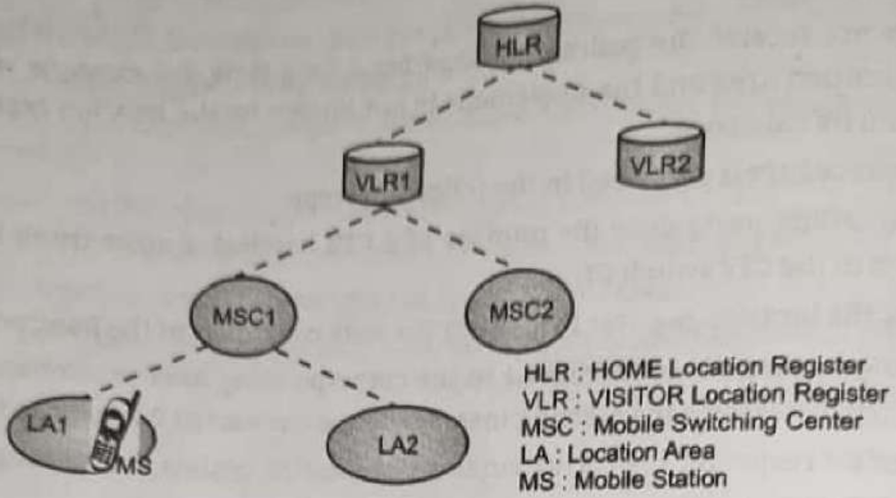

HLR
VLR1
VLR2
MSC1
MSC2
LA1
MS
LA2
HLR : HOME Location Register
VLR : VISITOR Location Register
MSC : Mobile Switching Center
LA : Location Area
MS : Mobile Station

Fig. 1.20

Step 1: The MS moves from LA1 to LA2, where both LAs are connected to the same MSC (Fig. 1.22) A location update request message is sent from the MS to the MSC through the BTS, include the address of the previously visited LA, MSC, and VLR TMSI is used to avoid sending the IMSI on the radio path

Step 2: The MSC forwards the location update request to the VLR by a TCAP message,

MAP_UPDATE_LOCATION_AREA

Address of the MSC

TMSI of the MS

Previous location area identification (LAI)

Target LAI

Other related information listed in Section 6.1.1 of GSM 09.02 and GSM 03.12

Step 3 and Step 4:

- MSC updates the LAI field of the VLR record, and replies with an acknowledgment to the MS through the MSC Fig. 1.21 Inter-LA registration message flow (See Fig. 1.21).

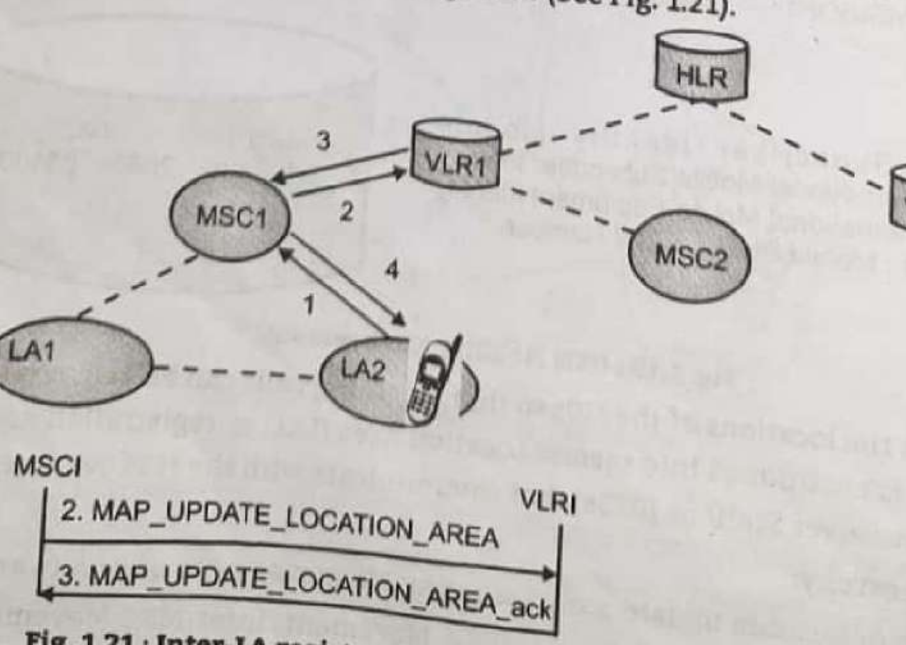


Fig. 1.21 : Inter-LA registration message flow Inter-MSC Movement

- Two LAs belong to different MSCs of the same VLR

  Steps 1 and 2: The location update request is sent from the MS to the VLR

  Step 3: VLR updates the LAI and the MSC fields of VLR record, and derives the HLR address of the MS from the MS's IMSI.

  VLR sends the **MAP_UPDATE_LOCATION** message to the HLR

  IMSI of the MS

  Address of the target MSC (i.e., MSC2)

  Address of the target VLR (i.e., VLR1)

  Step 4: HLR identifies the MS's record by using the received IMSI

  MSC number field is updated

  An acknowledgment is sent to the VLR

  Step 5 and 6: Similar to steps 3 and 4 in Inter-LA Movement

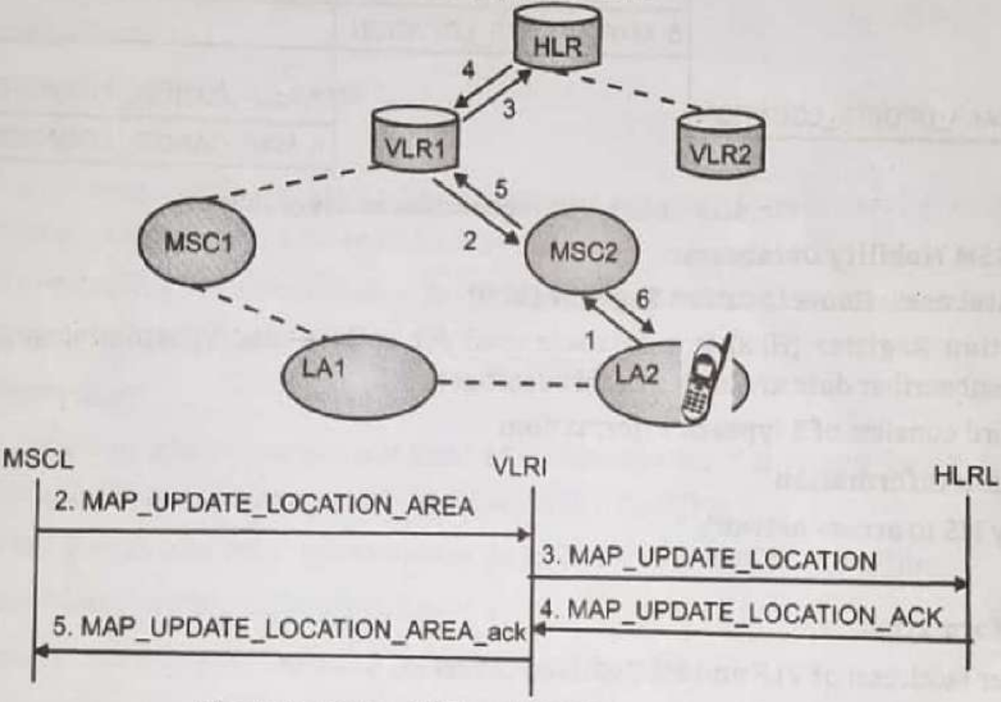

HLR
4
3
VLR1
VLR2
5
MSC1
2
MSC2
6
1
LA1
LA2
MSCL
VLRI
HLRL
2. MAP_UPDATE_LOCATION_AREA
3. MAP_UPDATE_LOCATION
4. MAP_UPDATE_LOCATION_ACK
5. MAP_UPDATE_LOCATION_AREA_ack

Fig. 1.22 : Inter –MSC registration message flow

Inter-VLR Movement

- Two LAs belong to MSCs connected to different VLRs

  Step 1: Location update request is sent from MS to VLR

  Step 2 and 3: VLR2 identifies address of the previous VLR(VLR1), then sends the message MAP_SEND_IDENTIFICATION to VLR1

  TMSI

  VLR1 sends IMSI to VLR2.

  Step 4 and 5: VLR2 creates a VLR record for the MS, and sends a registration message to update the HLR.

  HLR updates MSC and VLR address field of the record.

  An acknowledgment is sent back to VLR2.

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

  Step 7 and 8: The obsolete record of the MS in VLR1 is deleted.

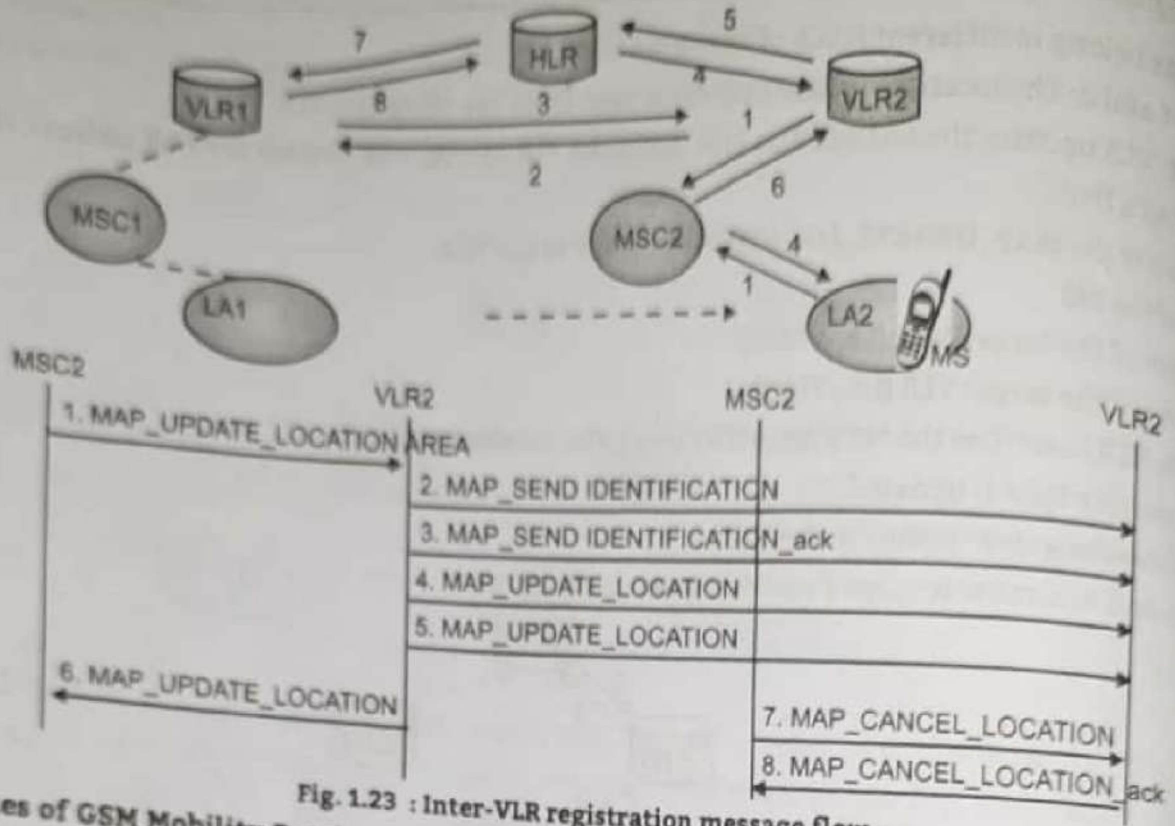


Fig. 1.23 : Inter-VLR registration message flow

Two Issues of GSM Mobility Databases:

1. **Mobility Databases: Home Location Register (HLR)**

- **Home Location Register** (HLR) is a database used for mobile user information management. All permanent subscriber data are stored in this database.
- An HLR record consists of 3 types of information:

(i) **Mobile Station Information**

- IMSI used by MS to access network
- MSISDN

(ii) **Location Information**

- ISDN number (address) of VLR and MSC where MS resides

(iii)**Service Information**

- Service subscription
- Service restrictions
- Supplementary services

2. **Visitor Location Register**

- Visitor Location Register (VLR) is a database of the service area visited by MS. All subscriber data of an MS required for call handling and other purpose are stored in VLR.

VLR Information Consists of 3 parts:

(i) **Mobile Station Information**

- IMSI
- MSISDN
- TMSI

(ii) **Location Information**

- MSC number
- Location Area ID (LAI)

(iii) Service Information

- Subset of the service information stored in the HLR

VLR Failure Restoration

- Service Information of a VLR record recovered by – The first contact between the VLR and the HLR of the corresponding MS.
- Location Information of a VLR record recovered by
  - First radio contact between the VLR and the MS
  - Mobile Station Information of a VLR record recovered by
  - Either by contact with the HLR or the MS
  - VLR record restoration is initiated by one of the three events
    1. MS registration
    2. MS call origination
    3. MS call termination.

VLR Record Restoration Initiation Event 1:

1. MS Registration:

- VLR considers the registration as inter-VLR movement because VLR record was erased by failure. VLR record is recovered from normal inter-VLR movement.
- MS is asked to send IMSI over the air because TMSI send from MS to the VLR cannot be recognized.

VLR Record Restoration Initiation Event 2:

2. MS Call Origination:

- VLR received the call origination request from MSC. Because the VLR record for MS is not found, VLR considers the situation as a system error "unidentified subscriber".
- The request is rejected, and MS is asked to initiate location registration procedure.

Call Termination Message (Failure Restoration):

VLR Record Restoration Initiation Event 3 – MS Call Termination:

Steps 1-3: Similar to the first three steps of basic call termination procedure, VLR is queried to provide the MSRN. Because searching for MS record by using IMSI fails, VLR creates a VLR record for MS Neither service nor location information is available, Steps 4 and 5 are executed in parallel.

Steps 4 and 7: VLR create MSRN using MSC number provide by MAP_PROVIDE_ROAMING_NUMBER message. MSRN is sent back to GMSC to set up call in step 8

Steps 5 and 6: VLR recovers service information of VLR record by sending **MAP_RESTORE_DATA** message to HLR. HLR sends the service information to VLR using **MAP_INSERT_SUBSCRIBER_DATA** message. Location information, specially LAI number will be recovered at step 11

Step 8: GMSC sends SS7 ISUP message IAM to target MSC.

Steps 9-11: MSC sends message MAP_SEND_INFO_FOR_INCOMING_CALL to VLR to obtain LAI information. VLR does not have LAI information, and sends. MAP_SEARCH_FOR_MOBILE_SUBSCRIBER to MSC to determine the LA of the MS. MSC initiates paging of the MS in all Las.

Steps 12 and 13: If paging is successful, the current LA address of the MS is sent back to VLR by MAP_PROCESS_ACCESS_REQUEST message

MAP_SEARCH_FOR_MOBILE_SUBSCRIBER is expensive because every BTS connected to the MSC mu perform the paging operation.

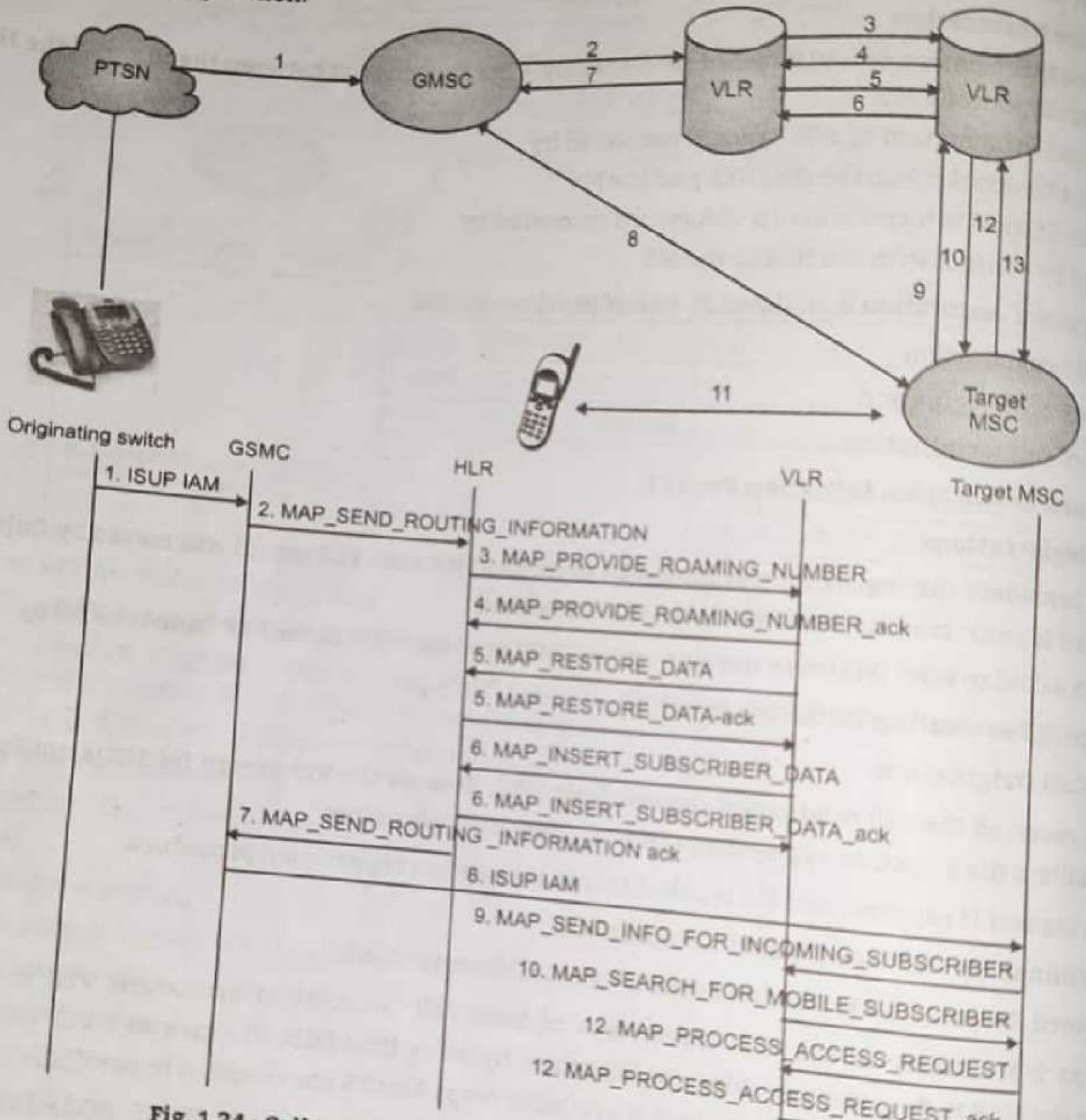

PTSN
1
GMSC
2
7
VLR
3
4
5
6
VLR
8
12
10
13
9
11
Target MSC
Originating switch
GSMC
HLR
VLR
Target MSC
1. ISUP IAM
2. MAP_SEND_ROUTING_INFORMATION
3. MAP_PROVIDE_ROAMING_NUMBER
4. MAP_PROVIDE_ROAMING_NUMBER_ack
5. MAP_RESTORE_DATA
5. MAP_RESTORE_DATA-ack
6. MAP_INSERT_SUBSCRIBER_DATA
6. MAP_INSERT_SUBSCRIBER_DATA_ack
7. MAP_SEND_ROUTING_INFORMATION ack
8. ISUP IAM
9. MAP_SEND_INFO_FOR_INCOMING_SUBSCRIBER
10. MAP_SEARCH_FOR_MOBILE_SUBSCRIBER
12. MAP_PROCESS_ACCESS_REQUEST
12. MAP_PROCESS_ACCESS_REQUEST_ack

Fig. 1.24 : Call termination message flow (failure restoration)

HLR Failure Restoration:

- It is mandatory to save the updates into non volatile storage. Changes of the service information are saved into the backup storage device immediately after any update.
- The location information is periodically transferred from the HLR into the backup. After an HLR failure, the data in the backup are reloaded into the HLR.
- HLR Restoration Procedure Message Flow.

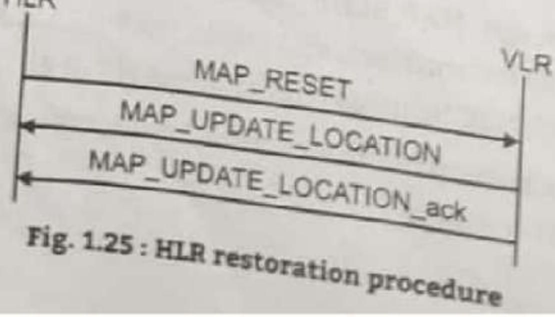


Fig. 1.25 : HLR restoration procedure

HLR Restoration Procedure:

- After an HLR failure, the data in the backup are reloaded into the HLR. An Uncovered Period = the time interval after the last backup operation and before the restart of the HLR.
- Data that have been changed in the uncovered period can not be recovered.

Step 1: The HLR sends an SS7 TCAP message MAP_RESET to the VLRs where its MSs are located.

Step 2: All the VLRs derive all MSs of the HLR. For each MS, they send an SS7 TCAP message, MAP_UPDATE_LOCATION, to the HLR.

- The HLR restoration procedure is not robust. – An MS may move into a VLR (which does not have any other MSs from the given HLR residing) during the uncovered period. – The new location is not known to the HLR at the last check-pointing time.
- If so, the HLR will not be locate the VLR of the MS during Step 1 of HLR restoration. VLR Identification Algorithm is to solve the problem.

Algorithm (VIA) (1/3):

- To simply the description, we assume that every VLR covers exactly one MSC. To implement VIA, extra data structures are required.
- In the backup, the extra data structure is a set VLR_List* of VLRs that have been modified during the uncovered period. After an HLR failure, the HLR only needs to send the MAP_RESET messages to VLRs listed in VLR

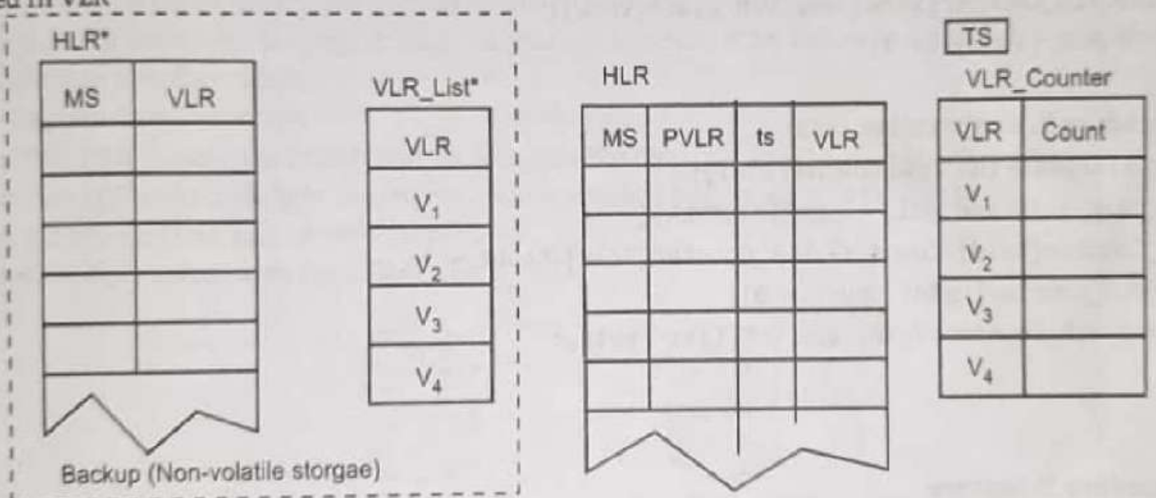


Fig. 1.26 : HLR architecture

- In HLR, every record includes two extra fields.

1. The ts field = the last time of location update
2. The PVLR field = the address of VLR where the resided at the last check-pointing time. Thus, for any MS p, we have

   HLR*[p].VLR = HLR[p].PVLR

- Two extra data structures are introduced in the HLR.

1. TS = the last check-pointing or backup time
2. VLR_Counter = {(VLR1,Count), (VLR2,Count), ..., (VLRn, Count)} where Count represents the "effective number" of MSs entering the VLR VLRn during the uncovered period.

- An MS is not effective to a VLR if it entered the VLR area then left the area during uncovered period.
- Note that the VLRs recorded in VLR_Counter are the VLRs in VLR_List*.

VIA Procedure 1: Check-Pointing

- In VIA, information of the HLR is periodically saved into the backup by this procedure.

  Step 1 : For every entry p in HLR* do:

  HLR[p]*.VLR <- HLR[p].VLR;

  Step 2 : TS <- current time;

Step 3 : For every location entry p in HLR do:
HLR[p].ts <- TS; HLR[p].PVLR <- HLR[p].VLR;

Step 4 : VLR_Counter <- NULL; VLR_List* <- NULL;

VIA Procedure 2: Registration (1/3)

Step 1. Update HLR:

```
Vold <- HLR[p].VLR;
Send message, MAP_CANCEL_LOCATION, to cancel the VLR entry of p at Vold;
HLR[p].VLR <- Vnew;
told <- HLR[p].ts;
HLR[p].ts <- t;
```

VIA Procedure 2: Registration (2/3)

Step 2 : Update the Vnew Count field in VLR_Counter:

```
If (HLR[p].VLR <> HLR[p].PVLR){
If (VLR_Counter[Vnew] exists){

VLR_Counter[Vnew].Count <-VLR_Counter[Vnew].Count+1;
}else{
create VLR_Counter[Vnew] and VLR_List*[Vnew];
VLR_Counter[Vnew] <- 1;
}  }
```

VIA Procedure 2: Registration (3/3)

Step 3 : Update the Vold counter entry:

```
If (told > TS and Vold <> HLR[p].PVLR){
VLR_Counter[Vold].Count <- VLR_Counter[Vold].Count - 1;
If (VLR_Counter[Vold].Count = 0){
Delete VLR_Counter[Vold] and VLR_List*[Vold];
}

}
```

VIA Procedure 3: Restore

Step 1 : TS <- current time;

Step 2 :

```
for (every location entry p in HLR){
HLR[p].PLVR = HLR[p].VLR <- HLR[p]*.VLR; HLR[p].ts <- TS;

}
```

Step 3 :

for (every VLR entry V in VLR_List*){
Send an SS7 TCAP MAP_RESET message to V;

VLR Overflow Control:

- The number of records in the VLR can change dynamically. It is possible that the number of the records in the corresponding VLR may be larger than that of the HLR, and the VLR may overflow if too many mobile users move into the LA in a short period.
- When a VLR is full, the incoming mobile users cannot register using the registration. To Solve the problem, overflow control algorithms O-I, O-II, O-III, and O-IV are presented.
- An extra flag (1 bit) is required in the HLR records.

Overflow Registration Operation:

- Fig. 1.27 shows overflow registration operation.

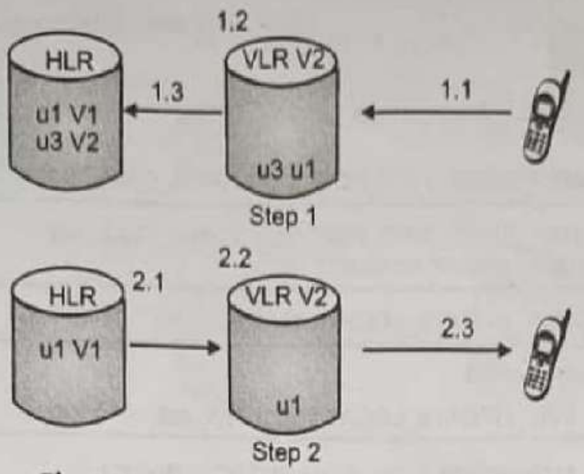


Fig. 1.27 : Overflow registration operation

Algorithm O-I: Registration

Step 1 : Registration Request:

Step 1.1 : Same as step 1 of the normal registration procedure

Step 1.2 : V2 is full. V2 follows a replacement policy to select a record to be deleted (u2in Fig. 1.28). The storage for the delete record is used to store u1's information. The selected user (i.e., u3) is called overflow user. The replacement policy may be based on various heuristics

Step 1.3 : V2 forwards the registration request to the HLR with indication that u3's record is delete due to database overflow Cont.

Step 2 : Registration Response:

Step 2.1 : HLR update the location of u1, and sets the overflow flag in u3's record

Step 2.2 : HLR acknowledges the registration operation and sends u1's profile to V2.

Step 2.3 V2 sends an acknowledgment to MS

Cancellation Operation with Overflow VLR

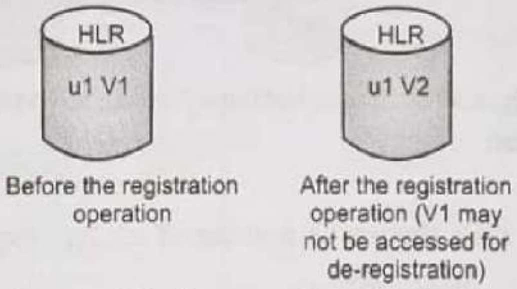

HLR
u1 V1
Before the registration operation
HLR
u1 V2
After the registration operation (V1 may not be accessed for de-registration)

Fig. 1.28 : Cancellation operation with overflow VLR

Algorithm O-II: Cancellation:

If u1 is an overflow user at V1, then u1 does not have a record in V1

Cancellation operation simply resets the overflow flag of u1's HLR record if u1is not an overflow user in V2.

Algorithm O-III: Call Origination:

Step 1: The MS sends the call origination request to V2

Step 2: V2 cannot fine u1'srecord, and denies the call request.

Steps 3 and 4: The MS initiates the registration procedure; Algorithm O-I is executed.

Steps 5 and 6: The MS reissues the call origination request, and the normal call origination procedure is executed.

Call Origination with Overflow VLR Call:

- Fig. 1.29 shows call origination with overflow VLR.

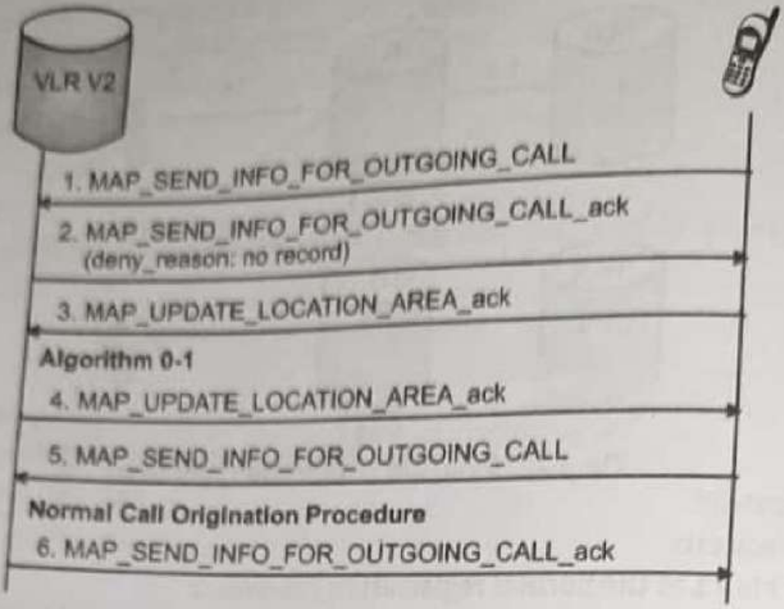

VLR V2
1. MAP_SEND_INFO_FOR_OUTGOING_CALL
2. MAP_SEND_INFO_FOR_OUTGOING_CALL_ack
(deny_reason: no record)
3. MAP_UPDATE_LOCATION_AREA_ack
Algorithm 0-1
4. MAP_UPDATE_LOCATION_AREA_ack
5. MAP_SEND_INFO_FOR_OUTGOING_CALL
Normal Call Origination Procedure
6. MAP_SEND_INFO_FOR_OUTGOING_CALL_ack

Fig. 1.29 : Call origination with overflow VLR

Termination with Overflow VLR:

- Fig. 1.30 shows call termination with overflow VLR.

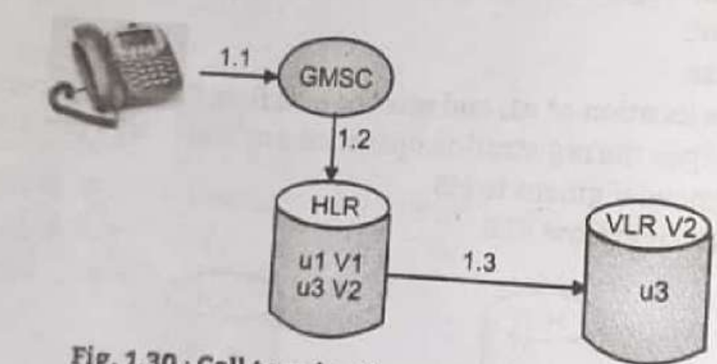


Fig. 1.30 : Call termination with overflow VLR

Algorithm O-IV: Call Termination

Step 1 : Location query:

Step 1.1 : The calling party dials the phone number of u1. The request is sent to the originatio switch in the PSTN.

Step 1.2 : The origination switch sends a location query message to the HLR

Step 1.3 : The HLR determines that u1 is an overflow user and sends a query message to obtain th routing information. The use profile information is attached in the message

Step 2 : Location response:

Step 2.1 : If V2 is not full, a record for u1 is created. If V2 is full, a user record is deleted and is used to store u1 and sends it back to HLR. V2 creates the routable address of u1 and sends it back to the HLR. If a record is replaced, the replacement information is included in the message

Step 2.2 : HLR returns the routable address to the originating switch. If a record is replaced, the overflow flags are updated at the HLR

Step 2.3 : The origination switch sets up the trunk to the MSC based on the routable address

Step 2.4 : The MSC pages the mobile phone and the call path is established

With Algorithms O-I through O-IV, an LA can accommodate an unlimited number of mobile users as long as the number of simultaneous phone calls to these users is no larger than the size of the database

Termination with Overflow VLR

- Fig. 1.31 shows call termination with overflow VLR.

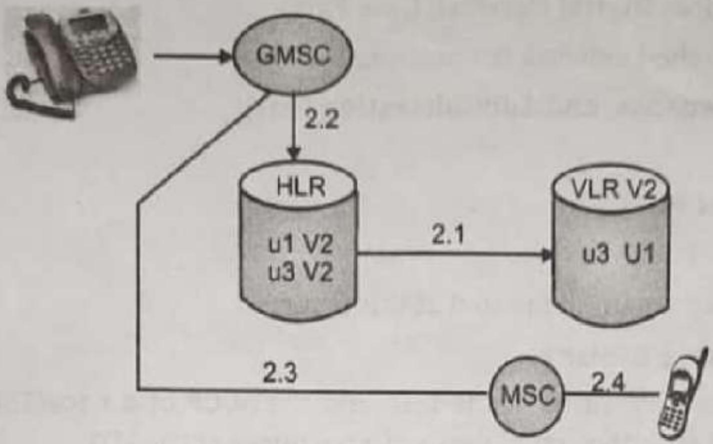


Fig. 1.31 : Call termination with overflow VLR

1.4 NETWORK SIGNALING

- To support PCS network management, protocols such as EIA/TIA Interim Standard 41 (IS-41 also known as ANSI-41) and Global system for Mobile communications (GSM), and Mobile Application Part(MAP) have been defined for PCS Network (PCN) intersystem operations.
- Interactions between a PCN and the PSTN are addressed in four aspects namely, Interconnection interfaces, Message routing, Mobility management and call control.

Signaling System No 7:

- PSTN is a signaling protocol. The interconnection between a PCN and the PSTN there are six types of SS7 signaling links.
- Two types, A-Link(access link) and D-Link (diagonal link).

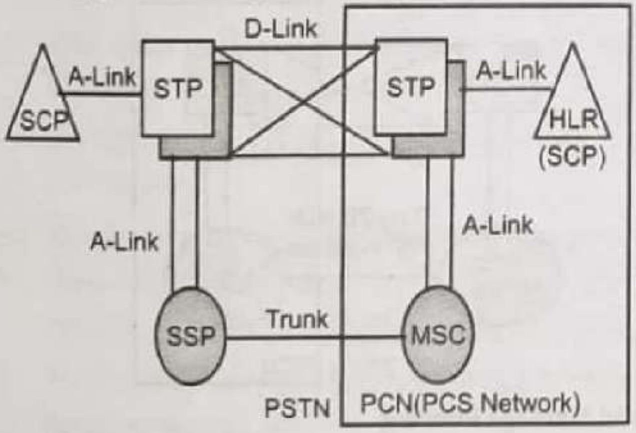


Fig. 1.32

■ SS7 protocol Layers

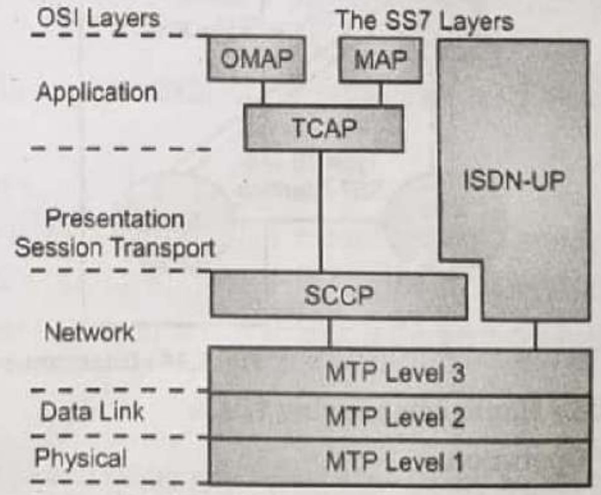


Fig. 1.33 : SS7 protocol Layers

MTP (Message Transfer Part) :

- Transfer signaling information
- MTP Level 2 provides reliable transfer of signaling message
- MTP Level 3 provides message routing and network management.

SCCP (Signaling Connection Control Part):

- Provides additional functions such as GTT to the MTP

TCAP (Transaction Capabilities Application Part):

- Provides the capability to exchange information between using noncircuit-related signaling.

ISUP-UP (Integrated Services Digital Network User Part):

- Establishes circuit-switched network connections

OMAP (Operations, Maintenance, and Administration Part):

- Application of TCAP.

MAP (Mobile APPLICATION Part):

- Application of TCAP
- Both IS-41 and GSM MAP are implemented at this layer.

Interconnection and Message Routing

- SS7 message routing is performed at the MTP and the SCCP of a node(SSP, STP or SCP). Signal messages are delivered with the actual destination address at the MTP.
- MTP level receives messages from TCAP, SCCP, ISUP. DPC(destination point code) of the mess uniquely identifies the destination node. Routing to the destination node is determined by the lo using lookup tables.

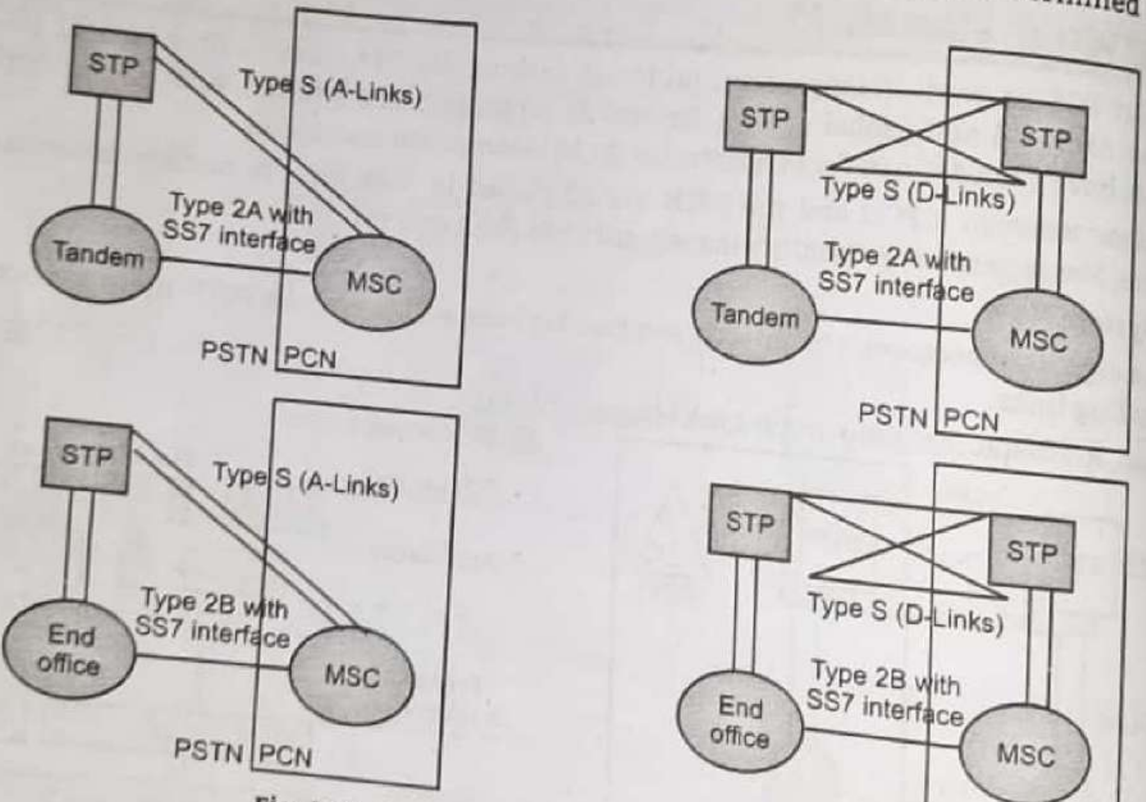


Fig. 1.34 : Interconnection and Message Routing

Mobility Management using TCAP:

TCAP Operation:

- More than 50 TCAP operation are defined.For three purposes : Inter-MSC handoff, automatic roaming, operations, administration and maintenance.
- TCAP message consists of two portions:
  1. Transaction portion-define package type
     Query with permission, Response
  2. Component portion-define number and types of components
     INVOKE, RETURN RESULT
     RETURN ERROR, REJECT

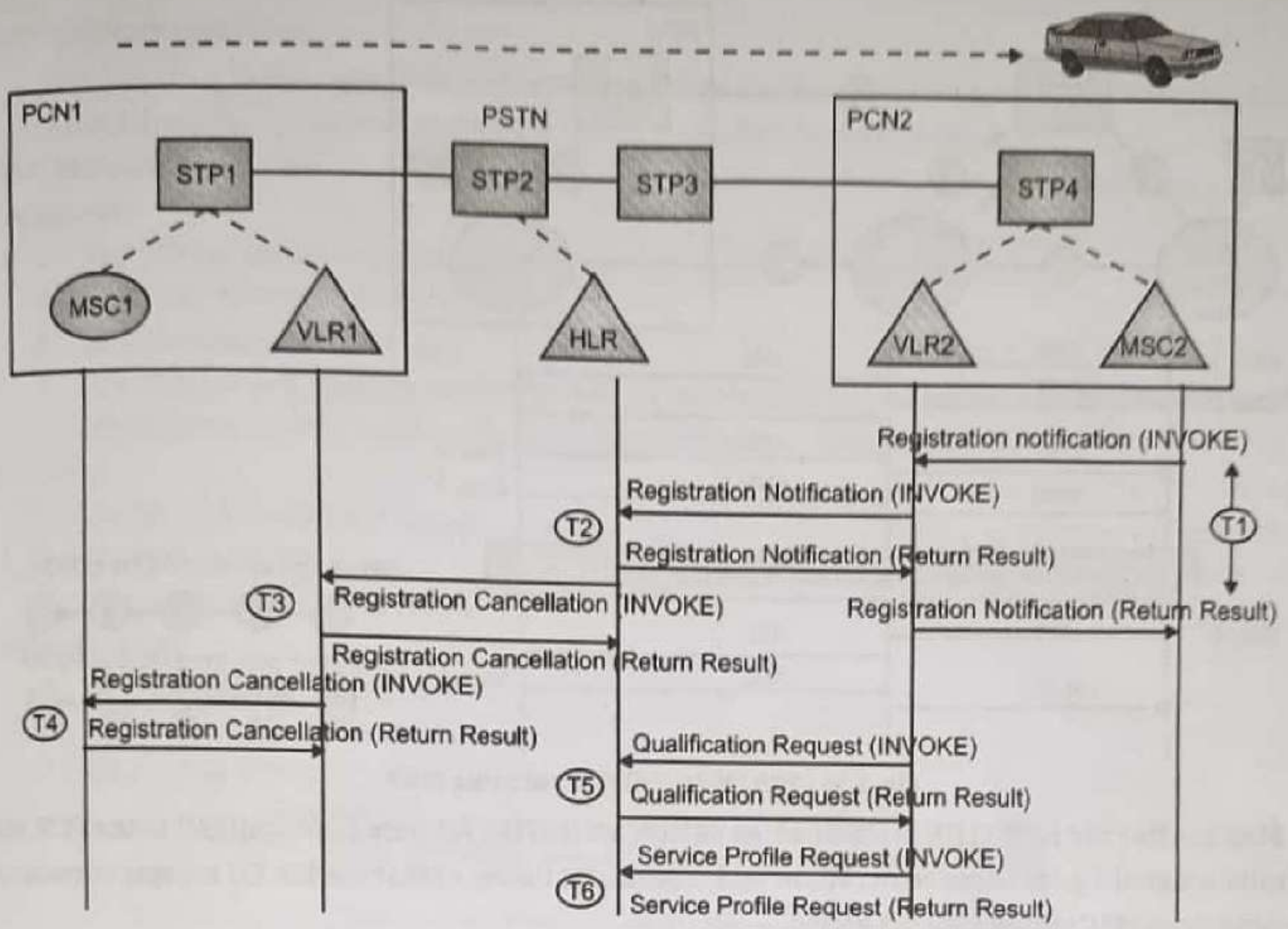

PCN1
PSTN
PCN2
STP1
STP2
STP3
STP4
MSC1
VLR1
HLR
VLR2
MSC2
Registration notification (INVOKE)
Registration Notification (INVOKE)
T1
T2
Registration Notification (Return Result)
T3
Registration Cancellation (INVOKE)
Registration Notification (Return Result)
Registration Cancellation (Return Result)
Registration Cancellation (INVOKE)
T4
Registration Cancellation (Return Result)
Qualification Request (INVOKE)
T5
Qualification Request (Return Result)
Service Profile Request (INVOKE)
T6
Service Profile Request (Return Result)

Fig. 1.35 : Mobility Management Using TCAP

IS-41 TCAP Message flow for MS Registration:

1. **Transaction 1** : When MS is in MSC2 service area, MSC2 sends a Registration Notification(INVOKE) to its VLR(VLR2).
2. **Transaction 2** : If MSC1 is net served by VLR2, then VLR2 sends a Registration Notification (INVOKE) to the MS's HLR.
3. **Transaction 3** : HLR sends a Registration cancellation (INVOKE) to the MS's previously visited VLR (VLR1).
4. **Transaction 4** : The cancellation propagates to MSC1
5. **Transaction 5** : After T2 is completed,VLR2 creates a registration record for MS. Sends a Qualification Request (INVOKE) to HLR to check MS's QUALIFICATION FOR RECEIVING SERVICES.
6. **Transaction 6** : VLR2 sends a service Profile Request (INVOKE) to HLR to obtain the service profile for the roaming MS.

PCN/PSTN Call Control Using ISUP:

Typical message flow for type 2A with SS7 land-to-mobile call setup and release involving a tandem switch:

- When MIN is dialed, end office(EO) notices that the number is for wireless service. Suppose that EO has HLR query capability.
- EO sends a query message to obtain MS's TLDN (Temporary Local Directory Number). Messages exchanged among switches, VLR and HLR are TCAP messages.

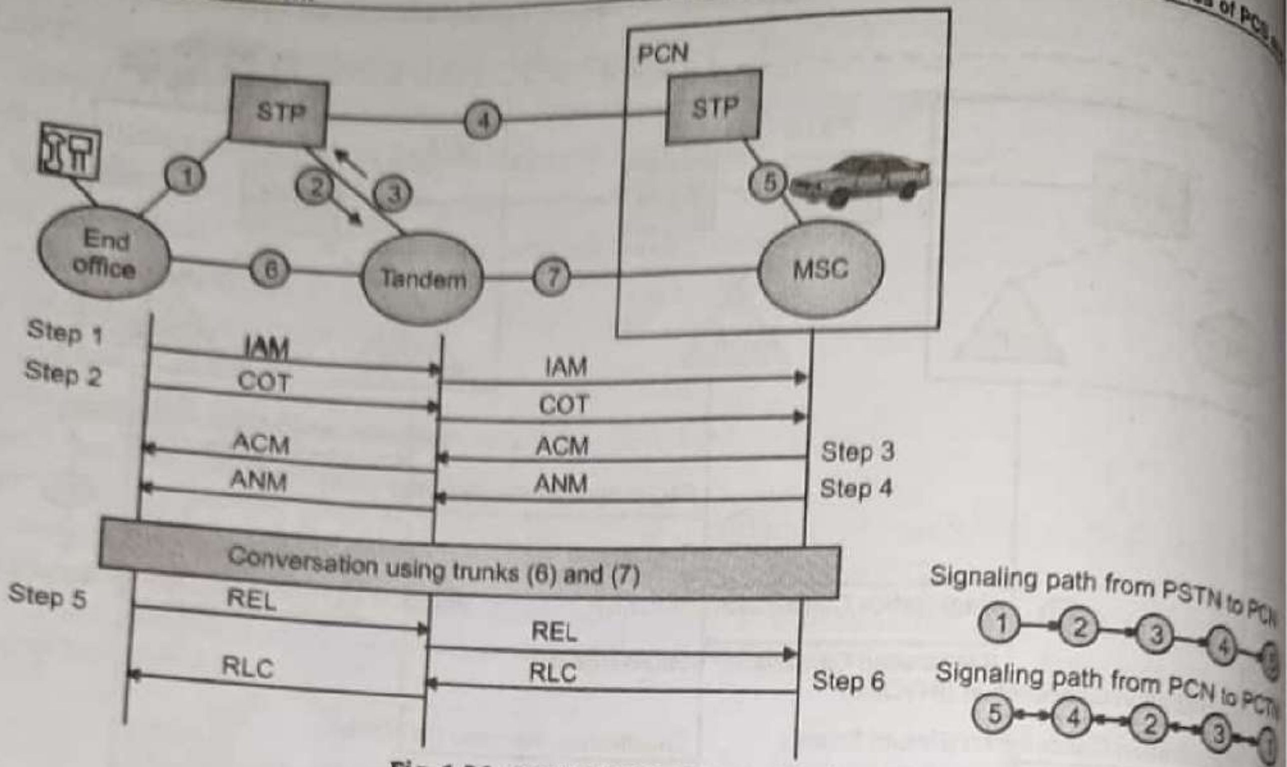


Fig. 1.36 : PCN/PSTN Call Control using ISUP

Step 1: After the MS's TLDN is obtained. eo SENDS AN INITIAL Address Message(IAM) to the PCN to initiate signaling for trunk setup. When IAM is sent, IAM timer is set at the EO. EO excepts to rece response from MSC within timeout period.

Step 2: If IAM sent from the EO to tandem specifies a continuity check, selected trunk from tande to EO. After continuity check is successfully completed, continuity message (COT) is sent from EO tandem, and trunk is set up. Same procedure could be performed when MSC receives IAM from tande

Step 3: When IAM arrives at MSC,MSC pages the MS.

- One of following three events occurs:

(a) MS is connected with another call:

- This situation is referred to as call collision Call is processed with call forwarding or call waiting MSC returns REL message to EO with a cause indicating the busy line situation.

(b) MS is idle:

- MSC send address complete Message (ACM) to EO. Message informs EO of MS information, charg indications, and end-to-end protocol requirements.
- When the EO receives the ACM, the IAM timer is stopped.

(c) MS does not answer the page:

- MSC returns REL message to EO.

Step 4: When MS answers call, An answer message (ANM) is sent from MSC to EO. Call is established through trunk path.

Step 5: EO sends a Release Message (REL) to indicate that specified trunk is being released from the connection. Trunk is not set to idle is EO until a RELEASE Complete Message(RLC) message is received.

Step 6: When MSC receives REL from EO, relies with a RLC. After RLC is sent, EO and tandem wait for 0.5 to 1 sec, before it seizes the released trunk for the next call.

GSM Network Signaling:

- GSM signaling defines the communications between the mobile and the network. Signaling has to be carried through the network and across the air- interface to the mobile.

GSM Protocol Interfaces:

Databases:

1. VLR (Visitor Location Register)
2. HLR (Home Location Register)
3. AUC (Authentication Center)
4. EIR (Equipment Identity Register):Used to maintain a list of legitimate, fraudulent. or faulty mobile stations also works with HLR to block calls from illegitimate MS.

Switches:

1. MSC (Mobile Switching Center)
2. GMSC (Gateway MSC)
3. SSP (Service Switching Point)

Radio Systems:

1. BSC (Base Station Controller)
2. BTS (Base Transceiver Station)
3. MS (Mobile Station)

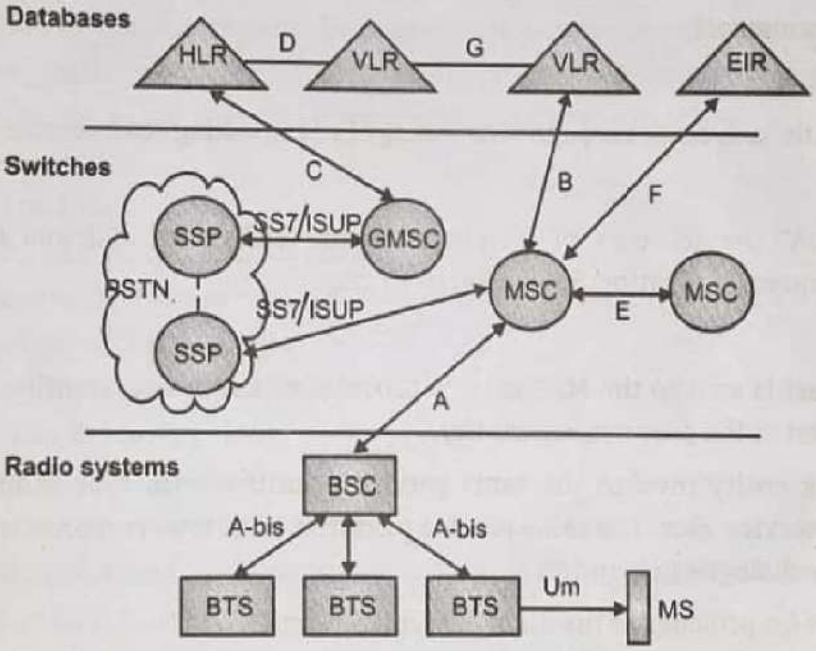


Fig. 1.37 : GSM Protocol Interfaces

GSM MAP Protocol Hierarchy:

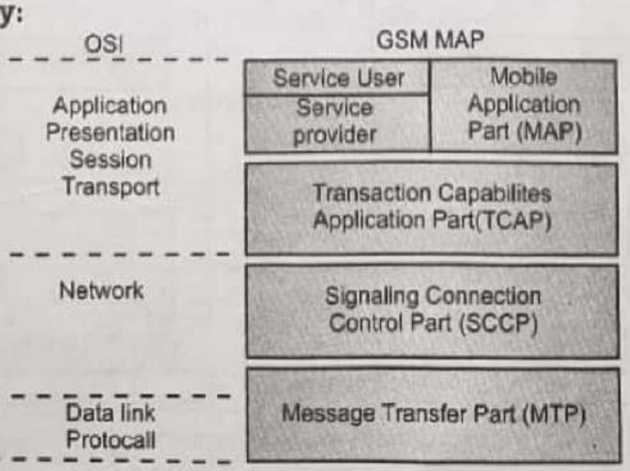

OSI
GSM MAP
Application
Presentation
Session
Transport
Service User
Service provider
Mobile Application Part (MAP)
Transaction Capabilites Application Part(TCAP)
Network
Signaling Connection Control Part (SCCP)
Data link Protocall
Message Transfer Part (MTP)

Fig. 1.38 : GSM MAP Protocol Hierarchy

- The Network entities may consist of several application service elements(ASEs)
- The SCCP addresses these ASEs with subsystem numbers (SSNs)

Table 1.2 : GSM MAP SCCP Subsystem Numbers

Application Service Element	Subsystem Number
HLR	00000110
VLR	00000111
MSC	00001000

Intra-GSM Network Message Delivery:

- The destination address of the message may be a simple destination point code (DPC) that ca used by the MTP for direct routing.

Inter-GSM Network Message Delivery:

- The origination node does not have enough knowledge to identify the actual address of destination. In this case, the SCCP translates the actual destination address by GTT (Global T Translation)

GSM MAP Service Framework:

GSM Network Entities:

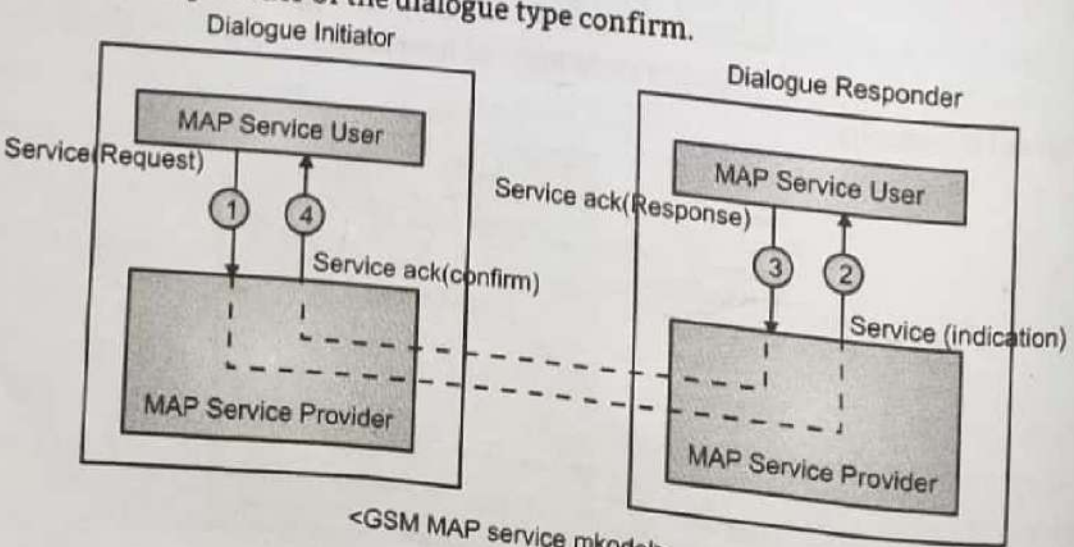
- Communicate with each other through MAP dialogues by invoking MAP service primitives.

Service Primitive:

- Initiated by a MAP service user of a network entity called the dialogue initiator. The servi primitives are Request, Indication, Response, confirm.

Procedure:

- The service request is sent to the MAP service provider of the network entity. The service provide delivers the request to the peer network entity.
- The peer network entity invokes the same service primitive with type indication to inform th destination MAP service user. The same service primitive with type response in invoked by the MA service user of the dialogue responder.
- After the MAP service provider of the dialogue type confirm.



<GSM MAP service mkodel>

Fig. 1.39 : GSM MAP service model

The Parameters of a Service Primitive Type:

M (Mandatory)

O (Service Provider Option)

U (Service User Option)

C (Conditional)

Two Type of MAP Services:

1. Specific MAP service
2. Mobility Services

Operation and maintenance services

Call-handling service

Supplementary service

Short message service management service

Common MAP Services:

- **MAP-OPEN :** Used to establish a MAP dialogue
- **MAP-CLOSE :** Used to clear a MAP dialogue
- **MAP-DELIMITER :** Used to explicitly request the TCAP to transfer the MAP protocol data units.
- **MAP-U-ABORT :** Used by the service user to abort a dialogue
- **MAP-P-ABORT :** Used by the service provider to abort a dialogue
- **MAP-NOTICE :** Used by the service provider to inform the service user of protocol problems such as abnormal event detected by the peer and response rejected by the peer.

MAP Protocol Machine:

DSM (Dialogue State Machine):

- Co-ordinates the Service State Machines (SSMs)
- For every MAP dialogue, an instance of DSM in created to handle the dialogue.

RSM (Requesting Service State Machine):

Handles a MAP-specific service requested.

PSM (Performing Service State Machine):

Handles a MAP service performed

Load Control:

- Monitors the traffic generated by the service activities. If overload situation in detected, low priority MAP operations may be ignored.
- Handoff, mobility management, short message services, subscriber –controlled inputs.

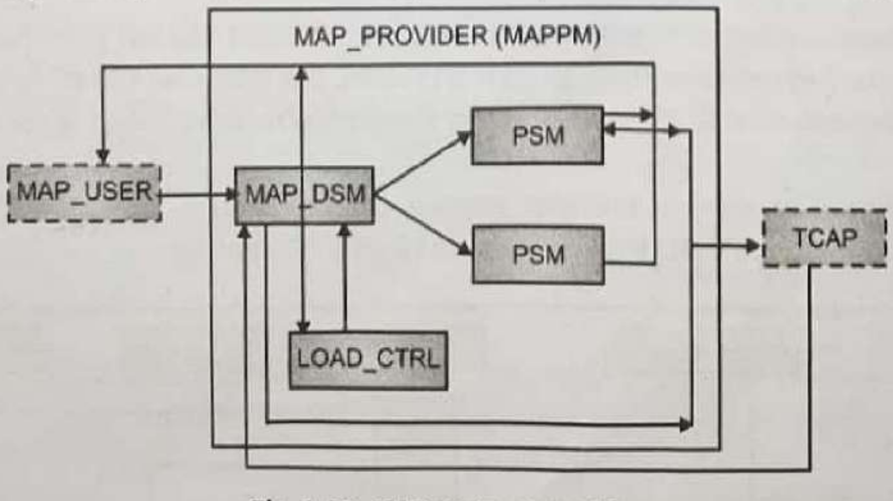


Fig. 1.40 : MAP protocol machine

MAP Dialogue:

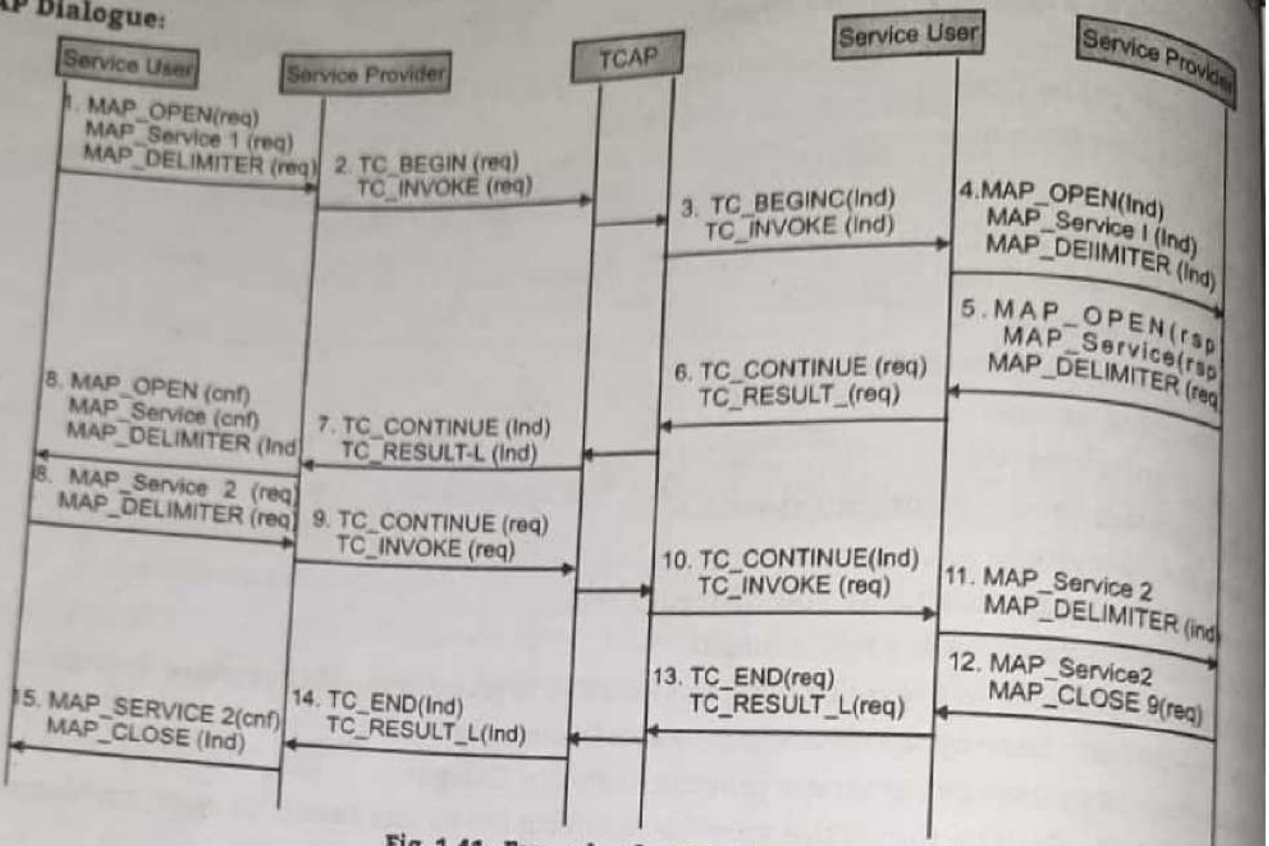
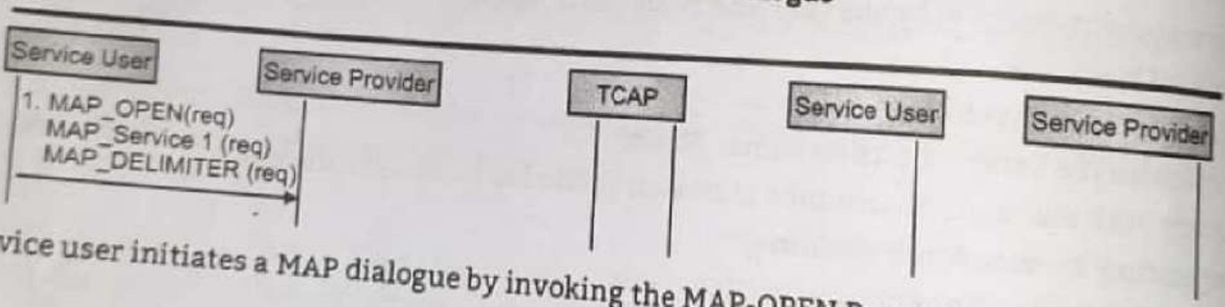


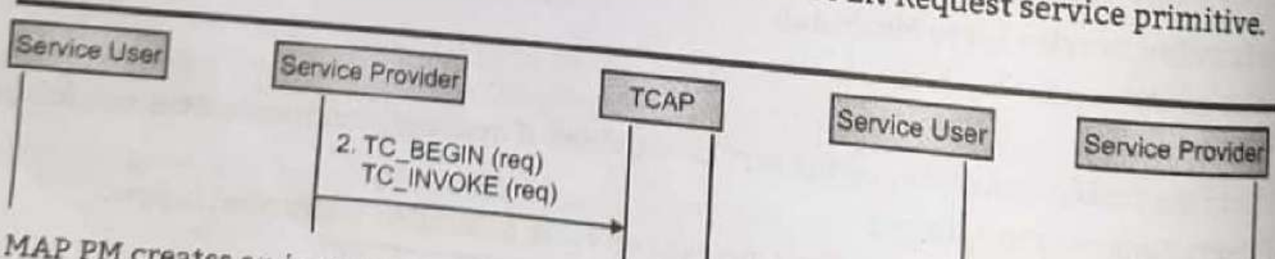
Fig. 1.41 : Example of MAP dialogue

Step 1 :



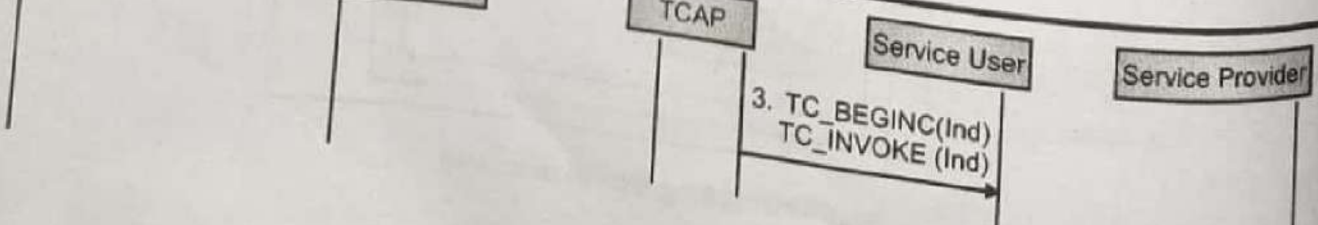
- A service user initiates a MAP dialogue by invoking the MAP-OPEN Request service primitive.

Step 2 :



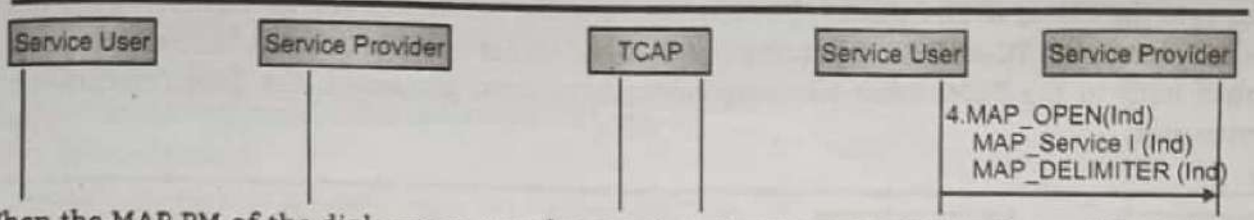
- The MAP PM creates an instance of DSM to handle the MAP-OPEN Request primitive. For every one of the following user request primitives, an RSM is created. The RSM uses the TC-INVOKE procedure to set the operation code and TCAP parameters for the service request. Then the control is passed back to the DSM.
- The DSM continues to process the user request primitives until the MAP-DELIMITER Request primitive is encountered. The MAP PM enables the TC-BEGIN primitive.

Step 3 :



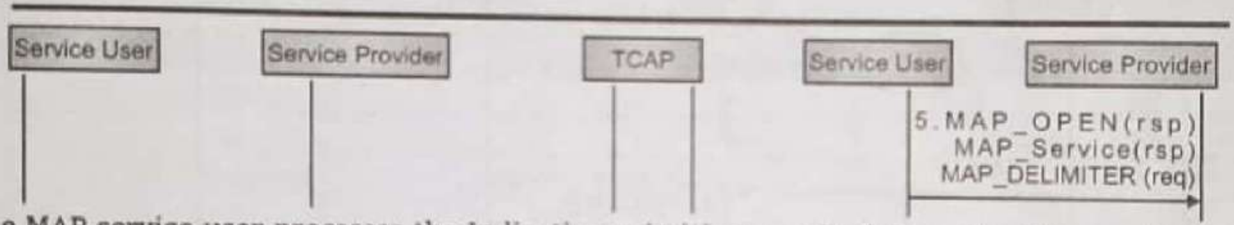
- The TC-* Request primitives will be delivered by the TCAP and the lower layer protocols of SS7 to the peer MAP PM;the primitives are now of type Indication.

Step 3 :



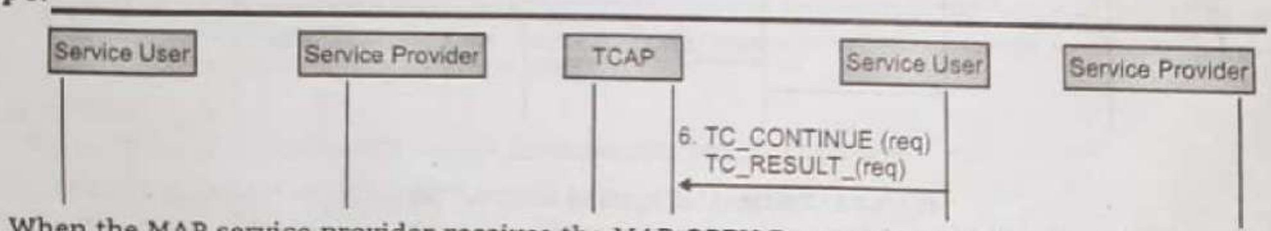
- When the MAP PM of the dialogue responder receives the TC-BEGIN Indication, a DSM is invoked. If the DSM identifies any error from the received TC-BEGIN Indication, a TC-U-ABORT Request is sent back to the dialogue initiator to terminate the dialogue.
- The DSM also checks if the system is overloaded. The DSM issues the MAP-OPEN Indication primitive to its MAP service user. The DSM then encounters the TC-INVOKE Indication primitive, which results in the creation of a PSM.
- The PSM sends a MAP-NOTICE to its MAP service user. No error occurs, the PSM issues a MAP- Service 1 Indication primitive to be passed to its service user, and the control is passed back to the DSM.
- After the DSM has processed all received components, it informs its MAP service user by the MAP-DELIMITER Indication primitive.

Step 4:



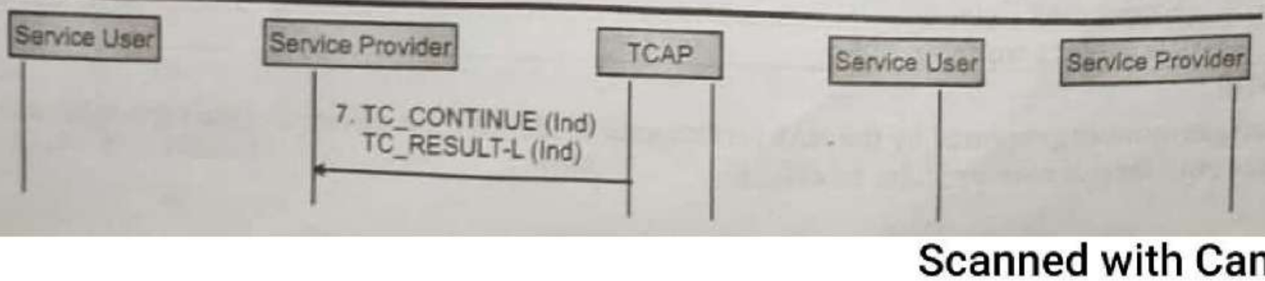
- The MAP service user processes the Indication primitives received from the MAP service provider, and returns the results with the MAP-OPEN and the MAP-Service 1 Response primitives, followed by the MAP-DELIMITER Request primitive.

Step 5:



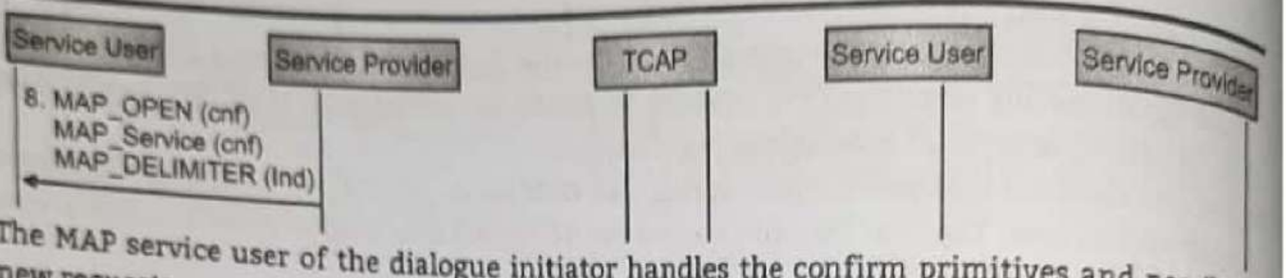
- When the MAP service provider receives the MAP-OPEN Response primitive, the DSM first checks if the response is negative. If so it generates a MAP_Refuse_PDU(protocol data unit) to be delivered by the Indication primitive TC-END. Assuming that the response is positive, a MAP_Accept_PDUis generated.
- The DSM proceeds to receive the MAP-Service1 Response primitive and passes the control to the PSM.
- The PSM checks if any user error is present. The PSM issues a TC-RESULT-L Request primitive and passes the control back to the DSM.
- The DSM continues to process the specific service primitives until the MAP-DELIMITER Request primitive is encountered. The DSM issues a TC-CONTINUE Request primitive with the MAP_Accept_PDU

Step 6:



- The TC-CONTINUE/TC-RESULT-L Indication primitives are received by the MAP service provider the dialogue initiator. When the DSM receives the TC-CONTINUE, it performs tests, as described step 4.
- It accepts the dialogue and passes the control to the RSM to handle the specific service primitive. The RSM maps the TC-RESULT-L parameters to the MAP-Service 1 confirm primitive and passes control back to the DSM. After all components have been processed, the DSM informs the service user.

Step 8:



- The MAP service user of the dialogue initiator handles the confirm primitives and possibly ma new requests.

MAP Service Primitives:

- Fig. 1.42 shows retrieval of routing information.

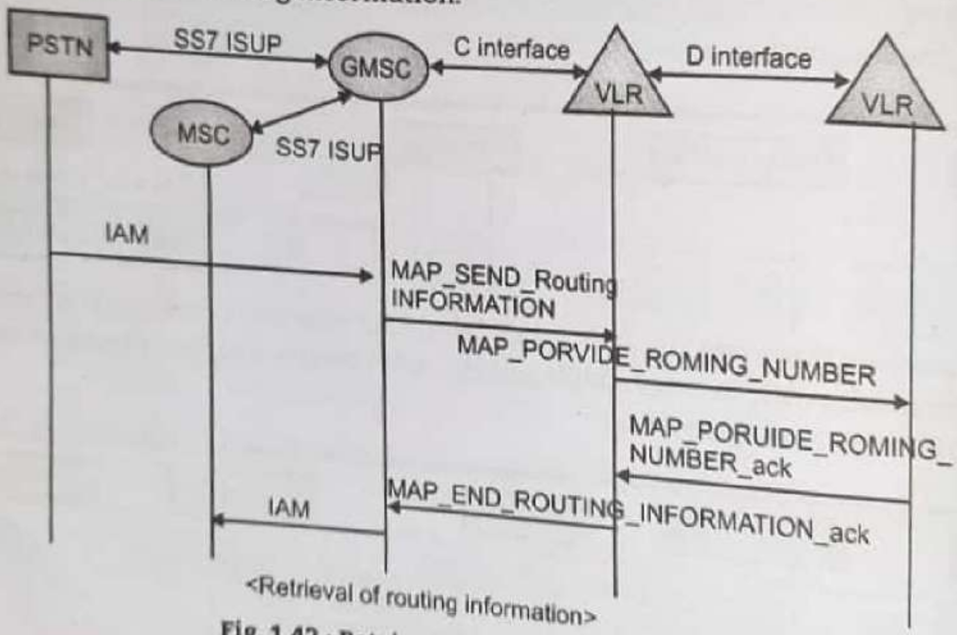

PSTN
SS7 ISUP
GMSC
C interface
VLR
D interface
VLR
MSC
SS7 ISUP
IAM
MAP_SEND_Routing INFORMATION
MAP_PORVIDE_ROMING_NUMBER
MAP_PORUIDE_ROMING_NUMBER_ack
IAM
MAP_END_ROUTING_INFORMATION_ack
<Retrieval of routing information>

Fig. 1.42 : Retrieval of routing information

Table 1.3 : MAP_SEND_ROUTING_INFORMATION Parameters

MAP_SEND_ROUTING_INFORMATION Parameters

Parameter Name	Request	Indication	Response	Confirm
Invoke ID	M	M(=)	M(=)	M(=)
MSSDN	M	M(=)		
CUG interlock	C	C(=)	C	C(=)
Number of Forwarding	C	C(=)		
Network Signal Info	C	C(=)		
IMSI			C	C(=)
MSRN			C	C(=)
Forwarding Data			C	C(=)
Provider Error				O

Invoke ID:

- A unique number generated by the MAP service user to identify the corresponding service primitive in the MAP service user-provider interface.

MSISDN:

- The mobile station ISDN number.

CUG (Closed User Group) Interlock:

- A group of users (eg. employees of a company) with specific network services. Possible to limit The incoming/outgoing calls inside the group.

CUG Outgoing Access:

- Represents the outgoing access of a closed user group.

Number of Forwarding:

- Counts the number of times the call has been forwarded.

Network Signal Info:

- Provides external signal information. Signaling protocol between the GSM network and the PSTN.

IMSI(International Mobile Subscriber Identity):

- Used to identify the called MS.

MSRN(Mobile Subscriber Roaming Number):

- The routing number that identifies the current location of the called MS.

Forwarding Data:

- Used to invoke the call-forwarding service.

User Error:

- Sent by the responder when an error is detected.

Table 1.4 : MAP_PROVIDE_ROAMING_NUMBER Parameters

Parameter Name	Request	Indication	Response	Confirm
Invoke ID	M	M(=)	M(=)	M(=)
IMSI	M	M(=)		
MSC Number	M	M(=)		
LMSI	C	C(=)		
GSM Bearer Capability	C	C(=)		
MSRN			C	C(=)
User Error			C	C(=)
Provider Error				O

MAP_PROVIDE_ROAMING_NUMBER Parameters:

MSC Number:

- The ISDN number of the MSC where the called MS resides.

LMSI(Local Mobile Station Identity):

- Used by the VLR for internal data management of the called MS.

GSM Bearer Capability:

- Included if the connection is for nonspeech services such as short message services.

User Error:

- Sent when an error is detected.

Practice Questions

1. What are the differences between cellular and low-tier PCS or cordless telephony?
2. What are the two major parts of a typical PCS network architecture?
3. What are the benefits of digital PCS systems?
4. What is the major difference between design for licensed and for unlicensed low-tier PCS systems?
5. What are the differences between the second generation mobile technology and third generation mobile technology?
6. What is handoff? What is roaming? How do you perform handoff during roaming?

7. Describe the main steps of inter-BS handoff procedure.
8. Describe the intersystem handoff procedure.
9. Why is path minimization necessary?
10. Draw the message flow of an MS originated call procedure.
11. Describe the basic PCS location update procedure.
12. Why is SS7 classified as a common channel signalling protocol? What are main elements in th SS7 architecture? Describe them.
13. At which level of the SS7 protocol stack does the GTT take place? When do we need GTT i mobility management? Can we modify IS-41 so that GTT is avoided?
14. What are the purposes of the package and the component types in a TCAP message?
15. What are the ISUP messages usually used for? Can we implement the IS-41 registratio procedure using ISUP?
16. Which layers are responsible for ISUP and TCAP routing? Do we need GTT for ISUP messag routing? Why or not.
17. Write features of GSM
18. State the various services offered by GSM system.
19. Draw and explain GSM system architecture.
20. Explain GSM radio subsystem.
21. List GSM air interface specification.
22. Explain channel types used in GSM in brief.
23. Explain Authentication process in GSM.
24. Describe call processing in GSM system with suitable diagram.
25. What is GSM Location update? When it is occurred?
26. Describe step procedure for VLR failure Restoration.
27. Write an algorithm for call termination of VLR overflow.
28. Write an algorithm for Registration of VLR overflow.
29. Explain Mobility Database of HLR and VLR
30. Explain HLR failure Restoration.
31. Describe step procedure for VLR failure Restoration.
32. Describe situation when GSM Location update is performed.
33. Describe the mobility of the database w.r.t HLR and VLR.
34. Describe the stepwise procedure for HLR Failure restoration.
35. Write an algorithm for call origination of VLR overflow.
36. Write an algorithm for call termination of VLR overflow.
37. Describe the registration process of mobile system when it is moving from one VLR to another VLR.
38. Describe GSM Location update procedure.
39. With neat diagram describe steps for VLR failure restoration procedure.
40. Write algorithm for call termination of VLR overflow.
41. Describe HLR restoration procedure.
42. What is the EIR used for in GSM networks?
43. Which network entities use GSM MAP to communicate with each other?
44. What are the four categories a service primitive can be?
45. What are the parts of the MAP protocol machine?
46. Why are there several instances of RSMs and PSMs in a MAP PM?
47. How is the routing information retrieved using GSM MAP?
48. Does GSM MAP use the same SS7 signaling mechanism as IS-41?

✤ ✤ ✤

2...

GPRS and Mobile Data Communication

Chapter Outcomes...

- Describe function of the given component of the GPRS architecture.
- Describe characteristics of the given IEEE protocol standard for wireless communication networks.
- Explain architecture of the given IEEE 802.11 protocol standard.
- Compare the performance of given wireless network technologies based on given criteria.
- State the procedure of scheduled maintenance of the given system.

Learning Objectives...

- To understand Basic Concepts of GPRS and its Architecture
- To learn Mobility Management and Routing in GPRS
- To learn WLAN, RFID, Bluetooth Technology, Wi-Max and Wi-Fi
- To study Mobile IP

2.0 INTRODUCTION

- The General Packet Radio Service (GPRS) is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks, e.g. to the Internet.
- It applies a packet radio principle to transfer user data packets in an efficient way between mobile stations and external packet data networks.
- The impressive growth of cellular mobile telephony as well as the number of internet users promises an exciting potential for a market that combines both cellular (mobile) service and data service.
- These services when combined is known as cellular wireless data services which can provide high-performance wireless internet access to the users.
- Existing cellular data services do not fulfill the needs of users and providers. From the user's point of view, existing cellular data services lags in-data rates are too slow, connection set up takes too long and is rather complicated, service is too expensive for most users.
- From the technical point of view, current wireless data services are based on circuit switched radio transmission. At the air interface, a complete traffic channel is allocated for a single user for the entire call period.
- In case of bursty traffic (eg. Internet traffic), this result in highly inefficient resource utilization. It is obvious that for bursty traffic, packet switched bearer services result in a much better utilization of the traffic channels.

- This is because a channel will only be allocated when needed and will be released immediately after the transmission of the packets. With this principle, multiple users can share one physical channel (statistical multiplexing).
- In order to address these inefficiencies, two cellular packet data technologies have been developed so far:
  1. Cellular digital packet data (CDPD) (for AMPS,IS-95,IS-136) and
  2. General Packet Radio Service (GPRS).
- GPRS was originally developed for GSM, but can also be integrated within IS-136.GPRS is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks, e.g., to the Internet.
- It applies a packet radio principle to transfer user data packets in an efficient way between GSM mobile stations and external packet data networks. Packets can be directly routed from the GPRS mobile stations to packet switched networks.
- Networks based on the Internet protocol (IP)(eg., the global Internet or private/corporate Intranets) and X.25 networks are supported in the current version of GPRS.

2.1 GPRS ARCHITECTURE AND GPRS NETWORK NODES

- General Packet Radio System is also known as GPRS is a third-generation step toward internet access. Fig 2.1 shows architecture of GPRS.

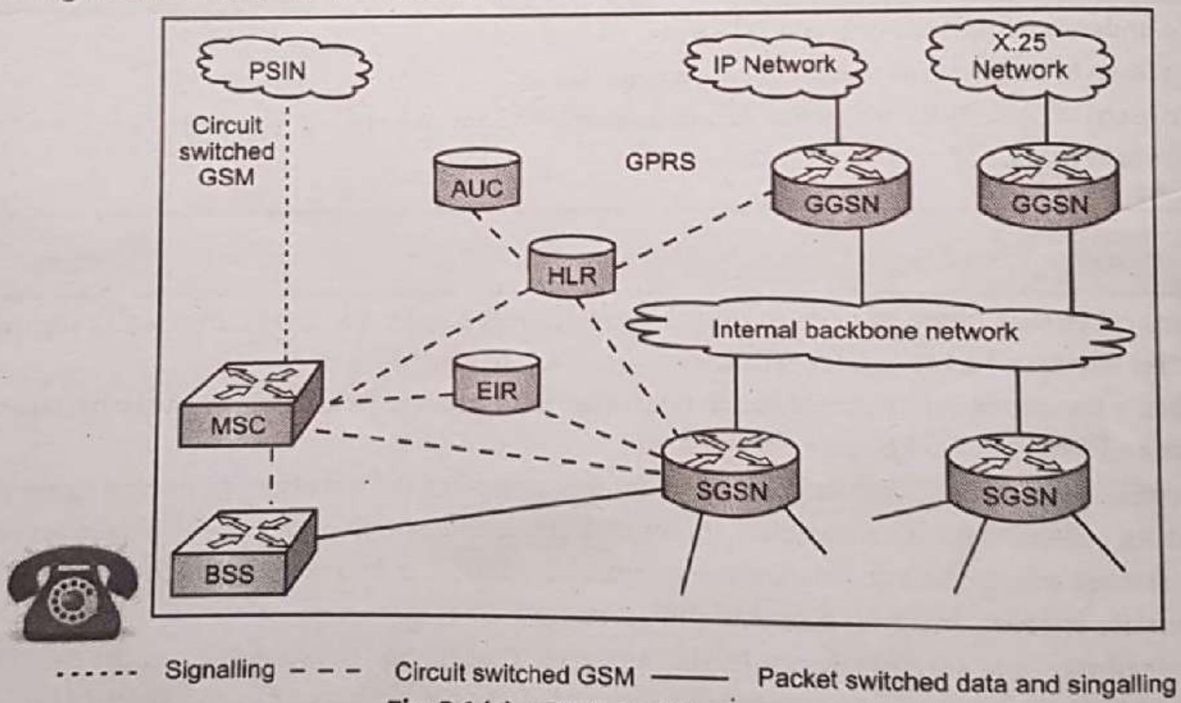


Fig. 2.1 (a) : GPRS Architecture

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission.
- This data network overlaps a second generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps.
- Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently. GPRS usually attempts to reuse the existing GSM network elements as much as possible.

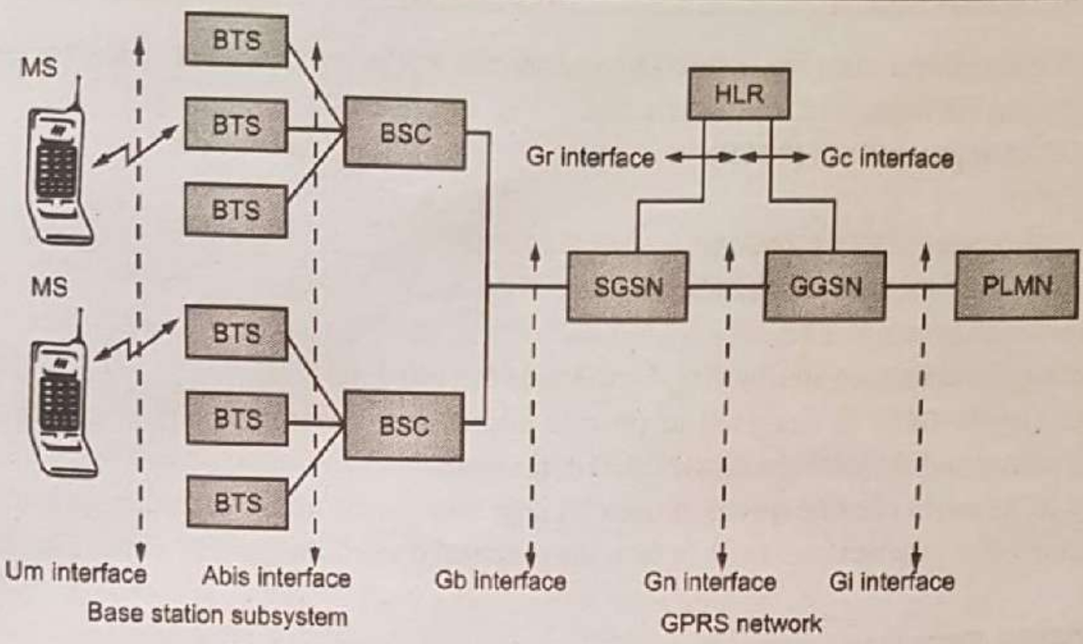


Fig. 2.1 (b) : GPRS Architecture with Network Nodes

- There are new entities called GPRS that supports nodes (GSN) which are responsible for delivery and routing of data packets between mobile stations and external packets networks.
- There are two types of GSNs namely; Serving GPRS Support Node (SGNS) and Gateway GPRS Support Node (GGNS).
- There is also a new database called GPRS register which is located with HLR. It stores routing information's and maps the IMSI to a PDN (Packet Data Network) address.

GPRS Mobile Stations:

- New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data.
- These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem:

- Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade.
- The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.
- When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call.
- However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes (GSN):

- A GSN is a network node which supports the use of GPRS in the GSM core network. All GSNs should have a GN interface and support the GPRS tunneling protocol. There are two key variants of the GSN, namely Gateway and Serving GPRS support node.
- Two new components are added namely, Called Gateway GPRS Support Nodes (GGSNs) and Serving GPRS Support Node (SGSN).

1. **Gateway GPRS Support Node (GGSN):**

- The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node.

- The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

2. **Serving GPRS Support Node (SGSN):**

- SGSN support:
  (i) Authentication of GPRS mobiles.
  (ii) Registration of mobiles in the network.
  (iii) Mobility management, and
  (iv) Collecting information on charging for the use of the air interface.
- At higher speeds GPRS is designed to provide packet-data services at higher speeds than those available with standard GSM circuit switched data services.
- In theory GPRS could provide speeds of upto 171 kbps over the air interface, although such speeds are never achieved in practical network. In fact, the practical maximum speed is a little over 100 kbps.

2.1.1 GPRS Services

- The GPRS provides a set of GSM services for data transmission in packet mode within a PLMN. In packet-switched mode, no permanent connection is established between the mobile and the external network during data transfer.
- Instead, in circuit-switched mode, a connection is established during the transfer duration between the calling entity and the called entity. In packet-switched mode, data is transferred in data blocks, called packets.
- When the transmission of packets is needed, a channel is allocated, but it is released immediately after. This method increases the network capacity. Indeed, several users can share a given channel, since it is not allocated to a single user during an entire call period.
- One of the main purposes of GPRS is to facilitate the interconnection between a mobile and the other packet-switched networks, which opens the doors to the world of the Internet.
- With the introduction of packet mode, mobile telephony and Internet converge to become mobile Internet technology.

GPRS Data Services:

- Wide range of corporate and consumer applications are enable by GPRS services. GPRS Service include all normal GSM services but in more efficient way.
- It also support services like E-mail, Web browsing, Enhanced short message, Wireless imaging with instant picture, Video service etc.

Document and Information Sharing

- A user is likely to use either of the two modes of the GPRS network. These are Application mode and Tunneling mode.

1. **Application Mode:**

- In this mode the user will be using the GPRS mobile phone to access the application running on the phone itself.
- The phone here acts as the end user devices. All GPRS phone have web browser as embedded application.
- This browser allows browsing of web sites. Some GPRS device support mobile execution environment.

2. **Tunneling Mode:**

- This mode is for mobile computing where the user will use the GPRS interface as an access to the network.

- The end user device will be a large footprint device like laptop computer or small footprint device like PDA's. The MS will be connected to the device and used as a modem to access the wireless data network.

GPRS Bearer Services:

- GPRS is a wireless extension of data networks. It can access to data networks, such as IP-based networks (public internet, private intranet, and IPv4 and IPv6 protocols) and X.25 based networks.
  1. **GPRS upgrades GSM Data Services and Provides the following Services :**
  2. **Point-to-Point (PTP) Service:** Internetworking with the Internet (IP protocols) and X.25 networks.
  3. **Point-to-Multipoint (PTM) Service:** Point-to-multipoint multicast and point-to-multipoint group calls.
  4. **SMS Service:** Bearer for SMS
  5. **Anonymous Service:** Anonymous access to predefined services.
  6. **Future Enhancements:** Flexible to add new functions, such as more capacity, more users, new accesses, new protocols, new radio networks.

2.1.2 GPRS Applications and Limitations

- In this section we will study GPRS applications and limitations.

Applications of GPRS:

1. **Mobility :** The ability to maintain constant voice and data communications while on the move.
2. **Immediacy :** Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.
3. **Localization :** Allows subscribers to obtain information relevant to their current location.

- GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times.

Limitations of GPRS:

1. Limited Cell Capacity for all users.
2. GPRS does impact a network's existing cell capacity. There are only limited radio resources that can be deployed for different uses.
3. Speeds much lower in reality.
4. Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight timeslots without any error protection.
5. Transit Delays GPRS packets are sent in all different directions to reach the same destination. This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link.

2.1.3 GPRS Quality of Service (QoS)

- Quality of Service (QoS) requirements of conventional mobile packet data applications are in assorted forms.
- The QoS is a vital feature of GPRS services as there are different QoS support requirements for assorted GPRS applications like real time multimedia, web browsing, and e-mail transfer.
- GPRS allows defining QoS profiles using the parameters like Service Precedence, Reliability, Delay and Throughput.
- These parameters are described below:

1. **Service Precedence:**

- The preference given to a service when compared to another service is known as Service Precedence. This level of priority is classified into three levels called as High, Normal and Low.
- When there is network congestion, the packets of low priority are discarded as compared to high or normal priority packets.

2. **Reliability:**

- This parameter signifies the transmission characteristics required by an application. The reliability classes are defined which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing, and corruption of packets.

3. **Delay:**

- The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the GI interface to an external packet data network.
- This includes all delays within the GPRS network, e.g., the delay for request and assignment of radio resources and the transit delay in the GPRS backbone network.
- Transfer delays outside the GPRS network, e.g., in external transit networks, are not taken into account.

4. **Throughput:**

- The throughput specifies the maximum/peak bit rate and the mean bit rate.
- Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session, depending on the QoS demand and the available resources.
- The billing of the service is then based on the transmitted data volume, the type of service, and the chosen QoS profile.

2.2 GPRS ARCHITECTURE AND GPRS NETWORK NODES

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. There are two key variants of the GSN, namely Gateway and Serving GPRS support node.

2.2.1 GPRS Network Nodes

- There are two Network Operation Nodes in GPRS:

1. GGSN:

- The first is the access point for an external data network and is known as the gateway GPRS support node (GGSN). It contains the routing for GPRS-attached users. With this information, GGSN is capable of delivering the packet data units (PDU) to the user's current access point.
- The location information can be obtained from the HLR via the optional Gc interface, The Gateway GPRS Support Node (GGSN) is a main component of the GPRS network.
- The GGSN is responsible for the interworking between the GPRS network and external packet switched networks, like the Internet and X.25networks.
- From the external networks' point of view, the GGSN is a router to a sub-network, because the GGSN 'hides' the GPRS infrastructure from the external network. When the GGSN receives data addressed to a specific user, it checks if the user is active.
- If it is, the GGSN forwards the data to the SGSN serving the mobile user, but if the mobile user is inactive, the data are discarded. On the other hand, mobile-originated packets are routed to the right network by the GGSN.

- To do all this, the GGSN keeps a record of active mobile users and the SGSN the mobile users are attached to. It allocates IP addresses to mobile users and last but not least, the GGSN is responsible for the billing.

2. SGSN:

- The second is the SGSN that serves the need of mobile users. When a user is GPRS-attached, the SGSN establishes a Mobility Management (MM) context containing information pertaining to routing, security and mobility, such as the identity of RA and LA where the MS is residing, and the MS's MM states, etc.
- The SGSN also ciphers PS traffic, given that the base transceiver station (BTS, in GPRS, BTS replaces the BS in GSM.) is only responsible to cipher CS traffic
- The Serving GPRS Support Node (SGSN) is a main component of the GPRS network, which handles all packet switched data within the network, e.g. the mobility management and authentication of the users. The SGSN performs the same functions as the MSC for voice traffic.
- The SGSN and the MSC are often co-located. The SGSN is connected to the BSC. The SGSN is the service access point to the GPRS network for the mobile user.
- On the other side the SGSN relays the data between the SGSN and relevant GGSN (and vice versa). The SGSN handles the protocol conversion from the IP used in the backbone network to the Sub-Network-Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) protocols used between the SGSN and the mobile users. These protocols handle compression and ciphering.
- The SGSN is also responsible for the authentication of GPRS mobiles. When the authentication is successful, the SGSN handles the registration of the mobile to the GPRS network and takes care of its mobility management.

2.2.2 Mobility Management in GPRS

- The main task of the mobility management is to keep track of the user's current location. The MS sends the location update message to the SGSN so that the network can be always aware of the current location of the MS.
- There are three states exist in the GPRS mobility management and the different location information is available in each state. As a result, the different mobility management strategies are applied in the different states.
- State Model By Performing a GPRS attach, the MS gets into READY state and if the MS does not transmit any packet for a long period of time until the READY timer is expired, the MS will get into STANDBY state.
- It is possible to transmit data only if the MS is in READY state, thus the MS in STANDBY state can switch back to the READY state, if a PDU transmission occurs and in the same way, at READY state if the GPRS detach is performed, the MS will be back into IDLE state and all PDP context will be deleted.
- The GPRS state model is shown in Fig. 2.2.
- In the STANDBY state, the MS sends the location update message seldom, so its location is not known exactly and the paging is necessary for every downlink packet, resulting in a significant delivery delay.
- In the READY state, the MS updates its location frequently. Consequently the MS's location is known precisely and no paging delay during delivery downlink packet. However this consumes much more the uplink radio capacity and battery of the MS.
- Location Update The State Model of GPRS Mobile Station deploys an appropriate location update strategy in order to maintain the optimum network capacity as well as the MS battery drain.
- Fig. 2.3 shows the fundamental concept of network cell-structure. Cell is the coverage area of the radio transmission of base station (BS).

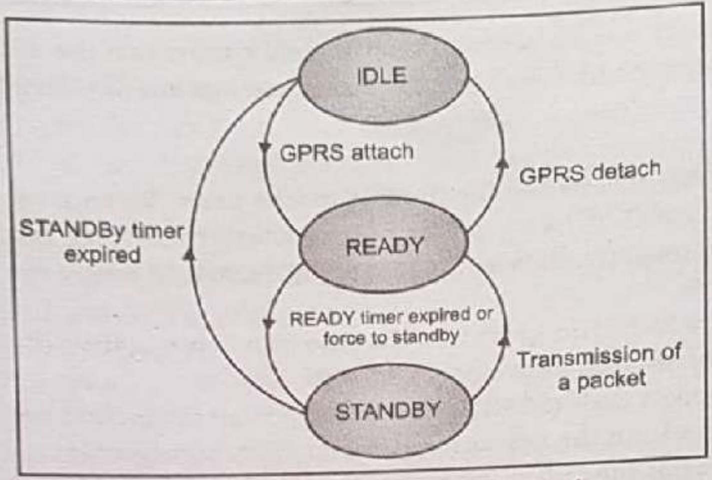


Fig. 2.2: State Model of GPRS Mobile Station

- Location Area (LA) and Routing Area (RA) consist of one or several cells and RA is always in one LA. When MS crosses LA border, a location update and RA update shall be done.
- In case MS moves within the same LA but crosses different RA, the RA update is needed. When the MS moves within the same LA and RA, cell update may be needed. It depends on the current state of the MS.
- The first case, that the MS updates the location every cell change, is used in READY state. This strategy ensures that the accurate location of the MS is always known and packet data can be delivered faster as no paging procedure is necessary.
- However the MS battery is drained more and uplink radio capacity is wasted for cell updates. The second case, used in STANDBY state, is that the MS updates the location only when the MS moves to a new Routing Area (RA).
- In this strategy, when data packet is sent to the MS, 10 paging is required in order to find out the current location of the MS. Thus, uplink capacity will be wasted for paging response and every downlink packet requires paging of the mobile delay.

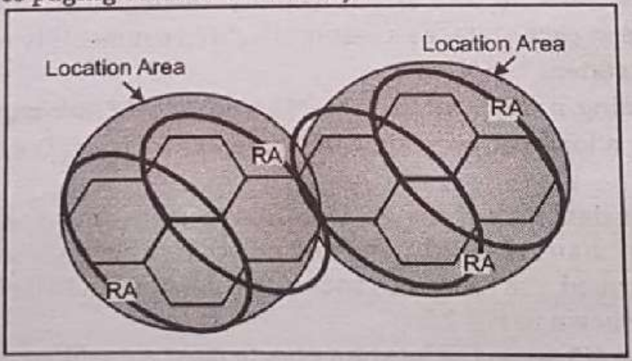


Fig. 2.3: Cell, Routing Area and Location Area

- RA Update Whenever the MS moves to a new RA, it sends a routing area update request including the routing area identity (RAI) of the old RA to its assigned SGSN. When the message arrives at the base station subsystem (BSS), the BSS adds the cell identifier (CI) of the new cell. Based on the RAI and CI data, the SGSN can derived the new RAI.
- Two different cases are possible; Intra-SGSN and Inter-SGSN routing area update.

1. **Intra-SGSN Routing Area Update:**

- The MS has moved to an RA, assigned to the same SGSN as the old RA.

- In this case, the SGSN knows already all necessary user profile, and can assign a new packet temporary mobile subscriber identity (P-TMSI) to the user without the need to inform other network elements.
- Fig. 2.4 shows the message exchange diagram of the IntraSGSN routing area update.

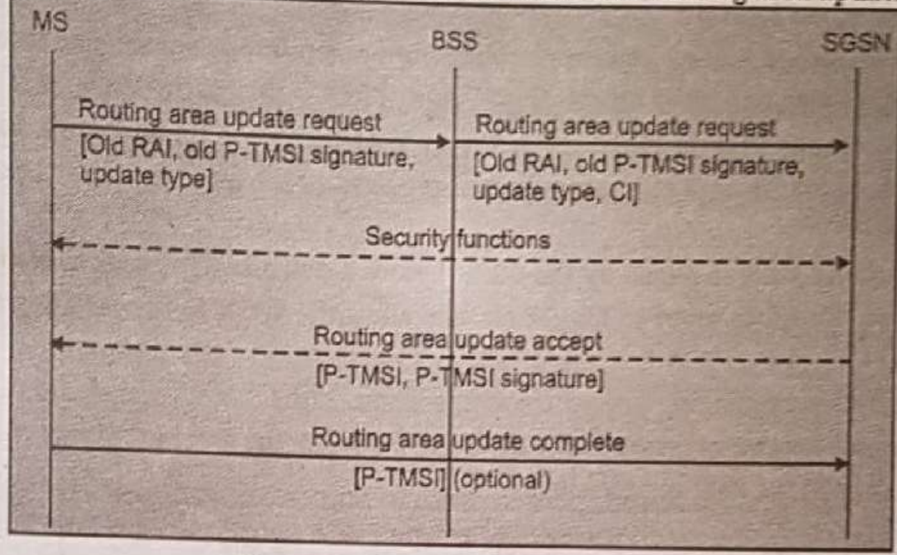

MS
BSS
SGSN
Routing area update request
[Old RAI, old P-TMSI signature, update type]
Routing area update request
[Old RAI, old P-TMSI signature, update type, CI]
Security functions
Routing area update accept
[P-TMSI, P-TMSI signature]
Routing area update complete
[P-TMSI] (optional)

Fig. 2.4: Intra-SGSN Routing Update

2. **Inter-SGSN Routing Area Update:**

- In this case, the MS has moved to an RA, assigned to a different SGSN, thus, the new SGSN does not have the user profile of the MS.
- The SGSN contacts the old SGSN and requests the PDP context of the user. After receiving the PDP context of the user, the new SGSN informs the involved network elements, such as the GGSN about the new PDP context of the user, and the HLR about the user's new SGSN, etc.
- Fig. 2.5 shows the message exchange diagram of the Inter-SGSN routing area update.

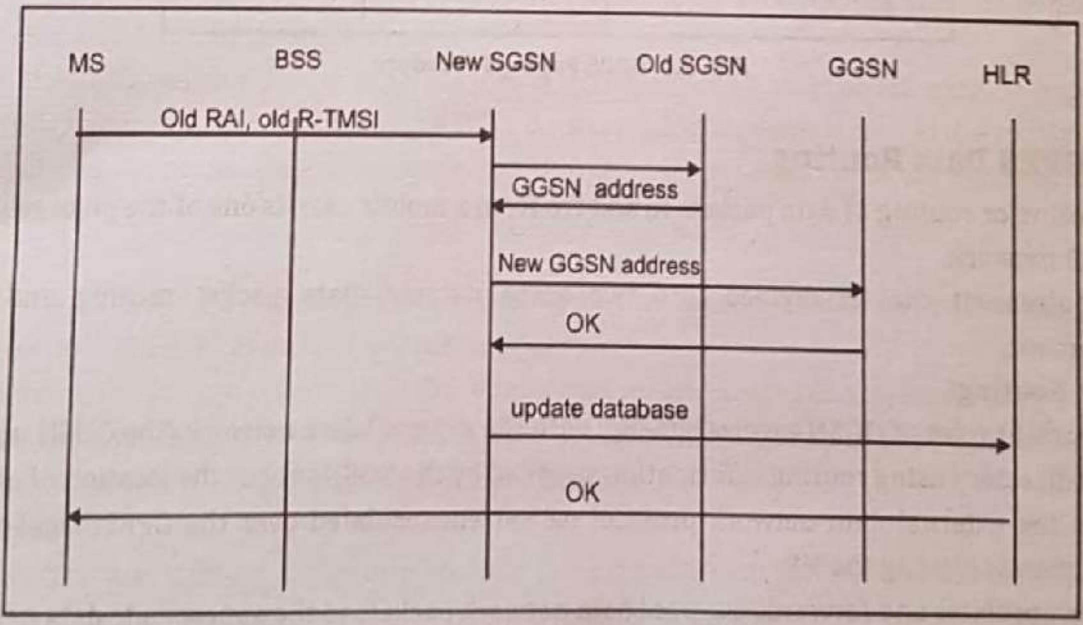


Fig. 2.5: Inter-SGSN Routing Area Update

- Cell Reselection When Mobile Station is in IDLE state, if the MS initiates attach procedure and the currently camped-on cell already supports GPRS then no cell reselection is required.
- On the other hand, if the currently camped-on cell does not support GPRS then a reselection procedure is required before execution of GPRS attach procedure.

- When MS is in STANDBY and READY state, it continuously monitors the surrounding cells. If the more suitable cell is found, a cell reselection procedure is performed. The cell reselection procedure in this case can be helpful to minimize the cell changes.
- Besides, when the MS moves to a new location, the cell reselection is needed to select a new cell most appropriate to the new location.
- While MS is in dedicated mode, then the changes from one cell to another is performed according to the network-controlled handover procedures.
- Paging of GPRS Mobile Station When the MS is in STANDBY state, the network does not know the precise location of MS, thus paging procedure is required to retrieve the accurate cell on which the MS has camped.
- The MS in STANDBY state is paged by the SGSN before a downlink transfer to that MS. The paging procedure cause the MS to move to READY state to allow the SGSN to forward downlink data to the radio resource.
- The SGSN supervises the paging procedure with a timer. If the SGSN receives no response from the MS to the Paging Request message, the SGSN will repeat the paging. Figure demonstrates the message exchange in the Paging procedure.

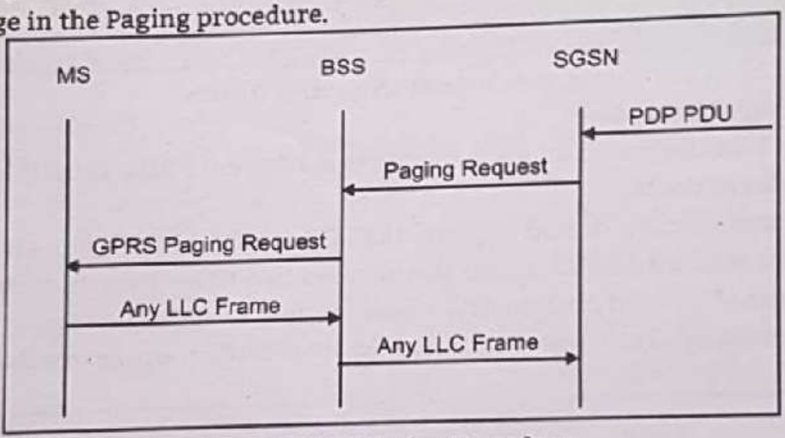


Fig. 2.6: GPRS Paging Procedure

2.2.3 GPRS Data Routing

- Data routing or routing of data packets to and fro from a mobile user, is one of the pivot requisites in the GPRS network.
- The requirement can be divided into two areas namely, Data packet routing and Mobility management.

Data Packet Routing:

- The important roles of GGSN involve synergy with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS.
- It routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS.
- It also decapsulates and forwards external data network packets to the appropriate data network and collects charging data that is forwarded to a charging gateway (CG).
- There are three important routing schemes:
  1. **Mobile-Originated Message :** This path begins at the GPRS mobile device and ends at the host and Network-initiated message when the MS is in its home network. This path begins at the host and ends at the GPRS mobile device.

2. **Network-Initiated Message when the MS Roams to another GPRS Network :** This path begins at the host of visited network and ends at the GPRS mobile device. The GPRS network encapsulates all data network protocols into its own encapsulation protocol called the GPRS tunnelling protocol (GTP). The GTP ensures security in the backbone network and simplifies the routing mechanism and the delivery of data over the GPRS network.
3. **Mobility Management:** The operation of the GPRS is partly independent of the GSM network. However, some procedures share the network elements with current GSM functions to increase efficiency and to make optimum use of free GSM resources (such as unallocated time slots).

   An MS can be in any of the following three states in the GPRS system. The three-state model is unique to packet radio. GSM uses a two-state model either idle or active.

Active State:

- Data is transmitted between an MS and the GPRS network only when the MS is in the active state. In the active state, the SGSN knows the cell location of the MS.
- Packet transmission to an active MS is initiated by packet paging to notify the MS of an incoming data packet. The data transmission proceeds immediately after packet paging through the channel indicated by the paging message.
- The purpose of the paging message is to simplify the process of receiving packets. The MS listens to only the paging messages instead of to all the data packets in the downlink channels. This reduces battery usage significantly.
- When an MS has a packet to transmit, it must access the uplink channel (i.e., the channel to the packet data network where services reside). The uplink channel is shared by a number of MSs, and its use is allocated by a BSS.
- The MS requests use of the channel in a random access message. The BSS allocates an unused channel to the MS and sends an access grant message in reply to the random access message.

Standby State:

- In the standby state, only the routing area of the MS is known. (The routing area can consist of one or more cells within a GSM location area).
- When the SGSN sends a packet to an MS that is in the standby state, the MS must be paged. Because the SGSN knows the routing area of the MS, a packet paging message is sent to the routing area.
- On receiving the packet paging message, the MS relays its cell location to the SGSN to establish the active state.

Idle State:

- In the idle state, the MS does not have a logical GPRS context activated or any Packet-Switched Public Data Network (PSPDN) addresses allocated.
- In this state, the MS can receive only those multicast messages that can be received by any GPRS MS. Because the GPRS network infrastructure does not know the location of the MS, it is not possible to send messages to the MS from external data networks.

Routing Updates:

- When an MS that is in an active or a standby state moves from one routing area to another within the service area of one SGSN, it must perform a routing update.
- The routing area information in the SGSN is updated, and the success of the procedure is indicated in the response message.
- A cell-based routing update procedure is invoked when an active MS enters a new cell. The MS sends a short message containing the identity of the MS and its new location through GPRS channels to its current SGSN. This procedure is used only when the MS is in the active state.

- The inter-SGSN routing update is the most complicated routing update. The MS changes from one SGSN area to another, and it must establish a new connection to a new SGSN.
- This means creating a new logical link context between the MS and the new SGSN and informing the GGSN about the new location of the MS.

2.2.4 Logical Channels in GPRS

- On top of the physical channels, a series of logical channels are defined to perform a multiplicity of functions, e.g., signaling, broadcast of general system information, synchronization, channel assignment, paging, or payload transport.
- Table 2.1 lists the packet data logical channels defined in GPRS. As with conventional GSM, they can be divided into two categories namely, Traffic Channels and Signaling (Control) Channels.

Table 2.1

Group	Channel	Function	Direction
Packet data traffic channel	PDTCH	Data traffic	MS◄►BSS
Packet broadcast control channel	PBCCH	Broadcast control	MS◄BSS
Packet common control channel (PCCCH)	PRACH	Random access	MS►BSS
	PAGCH	Access grant	MS◄BSS
	PPCH	Paging	MS◄BSS
	PNCH	Notification	MS►BSS
Packet dedicated control channels	PACCH	Associated Control	MS◄►BSS
	PTCCH	Timing advance control	MS◄►BSS

- The Packet Data Traffic Channel (PDTCH) is employed for transfer of user data. It is assigned to one MS (or in the case of PTM (point to Multipoint) to multiple mobile stations). One mobile station can use several PDTCHs simultaneously.
- The Packet Broadcast Control Channel (PBCCH) is a unidirectional point-to-multipoint signaling channel from the BSS to the MS. It is used by the BSS to broadcast specific information about the organization of the GPRS radio network to all GPRS mobile stations of a cell.
- Besides system information about GPRS, the PBCCH should also broadcast important system information about circuit switched services, so that a GSM/GPRS mobile station does not need to listen to the Broadcast Control Channel (BCCH).
- The Packet Common Control Channel (PCCCH) is a bidirectional point-to multipoint signaling channel that transports signaling information for network access management, e.g., for allocation of radio resources and paging. It consists of four sub-channels:
  (i) The **Packet Common Control Channel** (PCCCH) is used by the mobile to request one or more PDTCH.
  (ii) The **Packet Access Grant Channel** (PAGCH) is used to allocate one or more PDTCH to a mobile station.
  (iii) The **Packet Paging Channel** (PPCH) is used by the BSS to find out the location of a mobile station (paging) prior to downlink packet transmission.
  (iv) The **Packet Notification Channel** (PNCH) is used to inform a mobile station of incoming PTM messages (multicast or group call).
- The dedicated control channel is a bidirectional point-to-point signaling channel. It contains the channels PACCH and PTCCH.

- The Packet Associated Control Channel (PACCH) is always allocated in combination with one or more PDTCH that are assigned to one mobile station.
- It transports Signaling information related to one specific mobile station (e.g., power control information). The Packet Timing Advance Control Channel (PTCCH) is used for adaptive framc synchronization.
- The coordination between circuit switched and packet switched logical channels is important. If the PCCCII is not available in a cell, a mobile station can use the Common Control Channel (CCCH) of conventional GSM to initiate the packet transfer.
- Moreover. if the PI3CCH is not available, it will listen to the Broadcast Control Channel (BCCH) to get informed about the radio network.

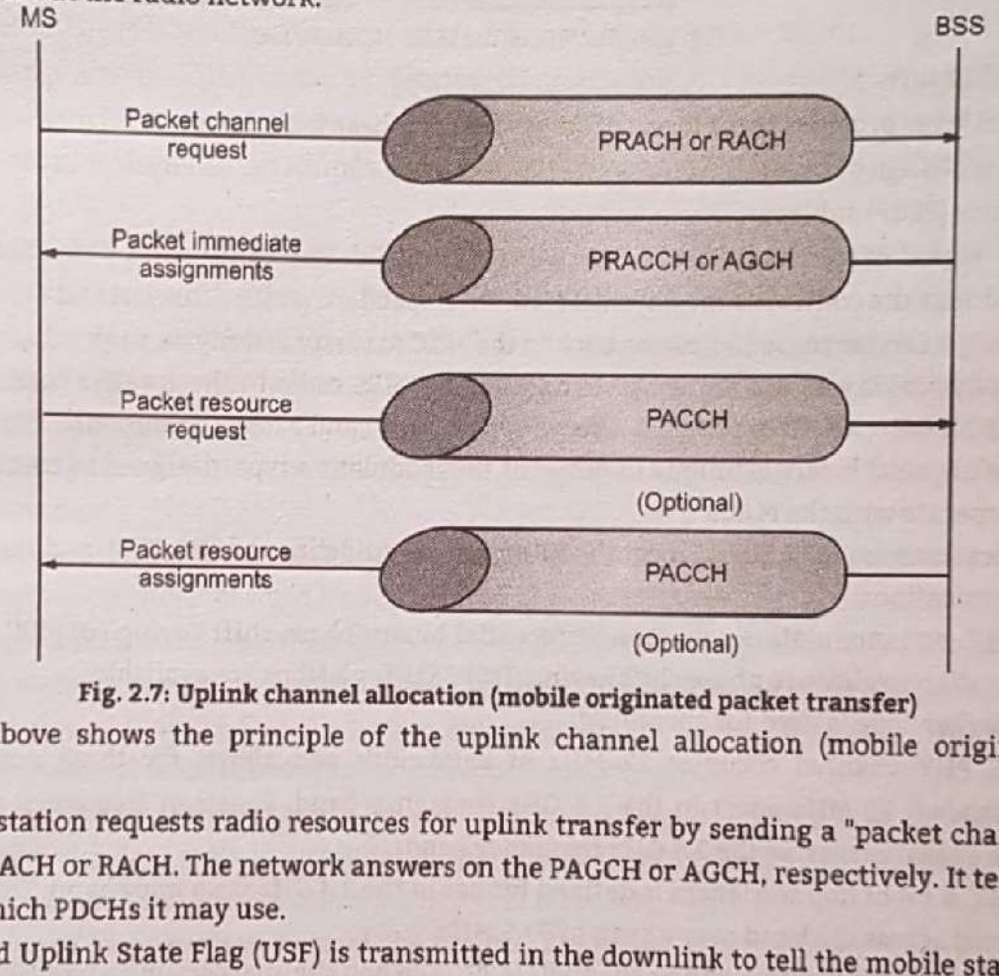


Fig. 2.7: Uplink channel allocation (mobile originated packet transfer)

- Fig. 2.7 above shows the principle of the uplink channel allocation (mobile originated packet transfer).
- A mobile station requests radio resources for uplink transfer by sending a "packet channel request" on the PRACH or RACH. The network answers on the PAGCH or AGCH, respectively. It tells the mobile station which PDCHs it may use.
- A so-called Uplink State Flag (USF) is transmitted in the downlink to tell the mobile station whether or not the uplink channel is free.

2.3 IEEE 802.11 WLAN STANDARDS AND RFID

2.3.1 IEEE 802.11 WLAN Standards

- The IEEE 802.11 committee is responsible for 'Wireless Local Area Network (WLAN)' standards. WLANs include IEEE 802.11a (WiFi 5), IEEE 802.11b (WiFi), IEEE 802.11g and IEEE 802.11n.
- The objective of the IEEE 802.11 standard was to define a Medium Access Control (MAC) sublayer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.
- The IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations.

- This type of architecture has several advantages. It is tolerant of faults in all of the WLAN equipment and eliminates possible bottlenecks a centralized architecture would introduce.

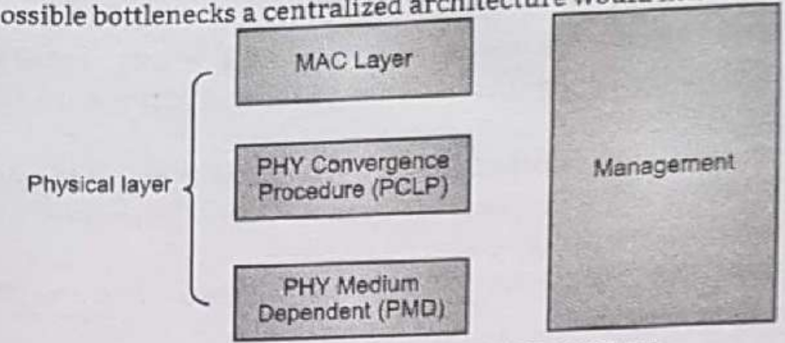


Fig. 2.8: OSI Model for IEEE 802.11 WLAN

802.11 Physical Layer:

- The physical layer provides three levels of functionality. These include:
  1. Frame exchange between the MAC and PHY under the control of the Physical Layer Convergence Procedure (PLCP) sublayer;
  2. Use of signal carrier and Spread Spectrum (SS) modulation to transmit data frames over the media under the control of the Physical Medium Dependent (PMD) sublayer; and
  3. Providing a carrier sense indication back to the MAC to verify activity on the media.
- The three physical layers are an IR baseband PHY, an FHSS radio in the 2.4 GHz band, and a DSSS radio in the 2.4 GHz. All three physical layers support both 1 and 2 Mbps operations.
- Each of the physical layers is unique in terms of the modulation type, designed to coexist with each other and operate with the MAC.
- The specifications for IEEE 802.11 meet the RF emissions guidelines of FCC, ETSI, and the Ministry of Telecommunications.
- In DSSS PHY, two modulation schemes, differential binary phase shift keying (DBPSK) - for 1 Mbps and differential quadrature phase shift keying (DQPSK) - for 2 Mbps are available.
- An 11-bit Barker code is used for spreading.
- Each DSSS PHY channel occupies 22 MHz of bandwidth and allows for three non-interfering channels spaced 25 MHz apart in the 2.4 GHz frequency band. Fourteen frequency channels are defined for operation across the 2.4 GHz frequency band.
- In FHSS PHY, a set of hop sequences is defined for use in the 2.4 GHz frequency band. The channels are evenly spaced across the band over a span of 83.5 MHz.
- In North America, the number of hop channels is 79. The hop channels occupy a bandwidth of 1MHz.

802.11a:

- It defines 'Orthogonal Frequency Division Multiplexing (OFDM)' scheme for modulation at the physical layer.
- The idea is to divide a channel into sub-channels, thus using multiple carriers. The modulation on each carrier is independent of each other.
- The OFDM PHY provides the capability to transmit PSDU frames at multiple data rates up to 54 Mbps for a WLAN where the transmission of multimedia content is a consideration.
- There are 48 data subcarriers and 4 carrier pilot subcarriers for a total of 52 nonzero subcarriers defined in IEEE 802.11a. Each lower data rate bit stream is used to modulate a separate subcarrier from one of the channels in the 5 GHz band.

802.11 Data Link Layer:

- The data link layer within 802.11 consists of two sublayers namely, Logical Link Control (LLC) and Media Access Control (MAC).

- The 802.11 uses the same 802.2 LLC and 48-bit addressing as the other 802 LAN, allowing for simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLAN.
- The sublayer above MAC is the LLC, where the framing takes place. The LLC inserts certain fields in the frame such as the source address and destination address at the head end of the frame and error handling bits at the end of the frame.
- MAC sublayer defines how a user obtains a channel when he or she needs one. The 802.11 MAC is similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it.
- The 802.11 MAC scheme includes 'Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)' to decide which station will access the media. 'Collision detection' cannot be used in WLANs.
- In IEEE 802.11, the MAC sublayer is responsible for asynchronous data service (e.g., exchange of MAC service data units (MSDUs), security service (confidentiality, authentication, access control in conjunction with layer management), and MSDU ordering.
- The MAC sublayer is also responsible for how a station joins an AP, switch to another AP.

802.11b-High Rate DSSS:

- In September 1999 IEEE ratified the 802.11b high rate amendment to the standard, which added two higher speeds (5.5 and 11 Mbps) to 802.11.
- To increase the data rate in 802.11b standard, advanced coding techniques are employed. Rather than the two 11-bit Barker sequences, 802.11b specifies complementary code keying (CCK).
- The 5.5 Mbps rate uses CCK to encode 4 bits per carrier, while the 11 Mbps rate encodes 8 bits per carrier. Both speeds use QPSK modulation and a signal at 1.375 Msps. This is how the higher data rates are obtained.
- The key contribution of the 802.11b addition to the WLAN standard was to standardize the physical layer support to two new speeds, 5.5 and 11 Mbps.
- To accomplish this, DSSS was selected as the sole physical layer technique for the standard, since frequency hopping cannot support the higher speeds without violating current FCC regulations.
- The implication is that the 802.11b system will interoperate with 1 Mbps and 2 Mbps 802.11 DSSS systems, but will not work with 1 Mbps and 2 Mbps FHSS systems.
- To support very noisy environments as well as extended ranges, 802.11b WLANs use dynamic rate shifting, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. Ideally, users connect at a full 11 Mbps rate.
- However, when devices move beyond the optimal range for 11 Mbps operation, or if substantial interference is present, 802.11b devices will transmit at lower speeds, falling back to 5.5, 2, and 1 Mbps.
- Likewise, if a device moves back within the range of a higher-speed transmission, the connection will automatically speed up again.Rate shifting is a physical layer mechanism transparent to the user and upper layers of the protocol stack.

802.11n:

- In response to growing market demand for higher-performance WLANs, the IEEE formed the task group 802.11n.
- The scope of this task group is to define modifications to the physical and MAC layer to deliver a minimum of 100 Mbps throughput at the MAC Service Access Point (SAP).
- 802.11n uses 'Multi-input Multi-output (MIMO)'. MIMO divides a bit stream into spatial streams, each directed towards a different antenna. This 'Space Division Multiplexing (SDM)' improves OFDM.

- The MIMO power saving mode mitigates to multipath only when it improves the overall performance of WLAN.
- The highest raw data rate will increase to 65Mbps from 54Mbps if the devices show compatibility with 802.11n standard.
- 'Beam forming' and 'Diversity' are two other techniques supported by 802.11n.
- Beam forming focuses the beam directly towards the intended antennas at the receiver.
- Diversity sums up the response of all antennas, takes the best subset, rejecting weak responses.
- 802.11n also supports aggregation. It bundles several frames and sends them together, reducing the total time required. This aggregation enhances the mixed mode operation offered by 802.11g.
- Doubling the channel width from 20MHz to 40MHz increases data rates. However, it is used by properly managing the needs of clients requiring high speeds and other clients which are connected to the network.
- The 802.11n specification was developed with previous standards in mind to ensure compatibility.

Table 2.2 : Primary IEEE 802.11 specifications and their comparisons

	802.11a	802.11b	802.11g	802.11n
Approval date	July 1999	July 1999	June 2003	August 2006
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK of OFDM
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5 GHz
Number of spatial streams	1	1	1	1, 2, 3 or 4
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz

2.3.1.1 WLAN Applications

- WLANs are designed to operate in Industrial, Scientific, and Medical (ISM) radio bands and Unlicensed-National Information Infrastructure (U-NII) bands. These bands are license free.
- Manufacturers have deployed WLANs for process and control applications.Retail applications have expanded to include wireless point of sale (WPOS).
- The health-care and education industry are also fast-growing markets for WLANs. WLANs provide high-speed, reliable data communications in a building or campus environment as well as coverage in rural areas. WLANs are simple to install.

WLAN Applications

- Public
  - Coffee shop
  - Airport
  - Convention Centre
- Private
  - Government
  - Enterprise
  - Manufacturing facility
  - Home
- **Semi-Public**
  - University
  - Hospital

2.3.1.2 IEEE 802.11 WLAN Architecture

- Fig. 2.9 shows WLAN architecture.

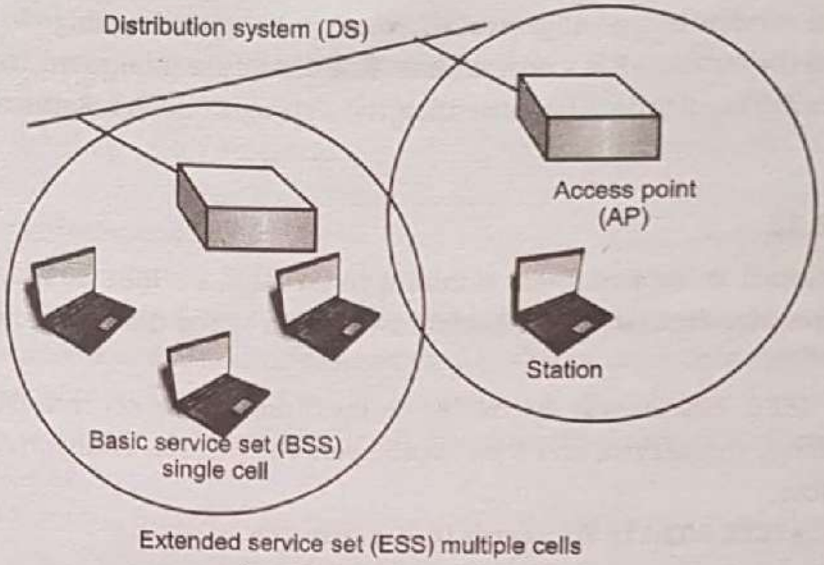


Fig. 2.9 : WLAN Architecture

STA: station

AP: access point

BSS: basic service set

ESS: extended service set

BSS: act as building blocks for formation of big wireless LANS

ESS: International collection of BSS

- When BSS's are interconnected the network becomes one with infrastructure. 802.11 infrastructure has several elements. Two or more BSS's are interconnected using a Distribution System or DS. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of Access Points (AP). An access point is a station, thus addressable.
- So, data moves between the BSS and the DS with the help of these access points.
- Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the Extended Service Set or ESS. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control Layer (LLC). This means that stations within the ESS can communicate or even move between BSS's transparently to the LLC.
- While the implementation for the DS is not specified, 802.11 does specify the services, which the DS must support. Services are divided into two sections namely, Station Services (SS) and Distribution System Services (DSS).
- There are five services provided by the DSS namely, Association, Reassociation, Disassociation, Distribution, Integration.
- The first three services deal with station mobility. If a station is moving within its own BSS or is not moving, the stations mobility is termed No-transition.
- If a station moves between BSS's within the same ESS, its mobility is termed BSS-transition. If the station moves between BSS's of differing ESS's it is ESS transition.
- Distribution and Integration are the remaining DSS's. Distribution is simply getting the data from the sender to the intended receiver.

- The message is sent to the local AP (input AP), then distributed through the DS to the AP (output AP) that the recipient is associated with. If the sender and receiver are in the same BSS, the input and out AP's are the same.
- So the distribution service is logically invoked whether the data is going through the DS or not. Integration is when the output AP is a portal. Thus, 802.x LANs are integrated into the 802.11 DS.
- Station services are Authentication, Deauthentication, Privacy and MAC Service Data Unit (MSDU) Delivery.

2.3.1.3 IEEE 802.11

- In 1997, IEEE developed an international standard for WLANs, i.e. IEEE 802.11. Like other IEEE 802 standards, this layer also focuses on the bottom two layers of the OSI model i.e. physical layer and data link layer.
- The objective of IEEE 802.11 was to define a medium access control (MAC) sublayer, MAC management protocol and service and 3 physical layers for wireless connectivity of fixed, portable and movable devices.

Comparison of Various IEEE 802.11x Standards (a/b/g/i/n etc):

Table 2.3

Parameters	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Applications	WLAN	WLAN	WLAN		
Modulation	DSSS , FHSS	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
Channel width	20 MHz	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Typical range	66 feet	75 feet	100 feet	150 feet	150 feet
Antenna configuration	1x1 SISO	1x1 SISO	1x1 SISO	1x1 SISO (Single Input-Single Output)	4x4 MIMO (Multiple Input-Multiple Output)

- IEEE 802.11i is mainly designed for enhanced security purposes. It addresses two main weaknesses of wireless security networks which are encryption and authentication. Encryption is accomplished by replacing WEP's original PRNG RC4 also by stronger cipher that performs three steps on every block of data.
- The authentication and key management is accomplished by the IEEE 802.1x standard.

2.3.2 Radio Frequency Identification (RFID)

- Radio frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data. The data is stored on and retrieved from RFID tags.
- The tag contains a transponder with a digital memory chip that is given a unique electronic product code. The data is written onto the memory and read from it.
- An RFID antenna packaged with a transceiver and decoder emits a signal activating the RFID tag so it can read and write data to the tag.

- When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the code ID of the tag and the data encoded in the tag's integrated circuit (silicon chip).
- In this way, an RFID tag is an information source. The data written onto it can be retrieved whenever needed or it can be transmitted to different RFID readers.
- RFID is also called dedicated Short Range Communication (DSRC).
- RFID components and their characteristics

RFID Features:

The following are the key features of RFID:

- **No Line-of-Sight:** To read or write RFID tags doesn't require line of sight.
- **Robust:** Because RFID systems do not need to be visible, they can be encased within rugged material protecting them from the environment in which they are being used. This means they can be used in harsh fluid and chemical environments and rough handling situations.
- **Read Speed:** Tags can be read from significant distances and can also be read very quickly. For example, on a conveyor.
- **Reading Multiple Items:** A number of tagged items can be read at the same time within an RF field. This cannot be done easily with visual identifiers.
- **Security:** Because tags can be enclosed, they are much more difficult to tamper with. A number of tag types now also come programmed with a unique identifier (serial identification) which is guaranteed to be unique throughout the world.
- **Programmability:** Many tags are read/write capable, rather than read only. This means that information can be written to the tag.

RFID Applications:

1. **Automotive:**

- Auto makers have added security and convenience to automobiles by using RFID technology for anti-theft immobilizers and passive entry systems.
- Some auto manufacturers use RFID systems to move cars through an assembly line. At each successive stage of production, the RFID tag tells the computers what the next step of the automated assembly is.

2. **Animal Tracking:**

- Ranchers and livestock producers use RFID technology to meet export regulations and optimize livestock value.
- Wild animals are tracked in ecological studies, and many pets who are tagged are returned to their owners.
- Thus a tag can carry information as simple as a pet owner's name and address.

3. **Assets Tracking:**

- Hospitals and pharmacies meet tough product accountability legislation with RFID; libraries limit theft and keep books in circulation more efficiently.

4. **Contactless Commerce:**

- Blue-chip companies such as American Express, Exxon Mobile, and MasterCard use innovative form factors enabled by RFID technology to strengthen brand loyalty and boost revenue per customer.

5. **Supply chain:**

- Wal-Mart, Target, Best Buy, and other retailers have discovered that RFID technology can keep inventories at the optimal level, reduce out of stock losses, limit shoplifting, and speed customers through check-out lines.

6. **Replacement for Bar Codes:**

- RFID can serve a lot of advantages by replacing bar codes.
- One of the key differences between RFID and bar code technology is RFID eliminates the need of line-of-sight reading that bar coding depends on.
- Also, RFID scanning can be done at greater distances than bar code scanning. High frequency RFID systems (850–950 MHz, 2.4–2.5 GHz) offer transmission ranges more than 90 feet.
- Barcodes are fixed at the time of printing and can be rendered useless by defacement or smudging. Bar codes can be spoofed or easily defeated by any malicious individual having a laser printer at their disposal.

2.3.2.1 Different Components of RFID and Communication Among The Components

- Radio frequency identification (RFID) is an automatic identification method, based on storing and remotely retrieving data using devices called RFID tags or transponders. Fig 2.10 shows schematic of RFID.

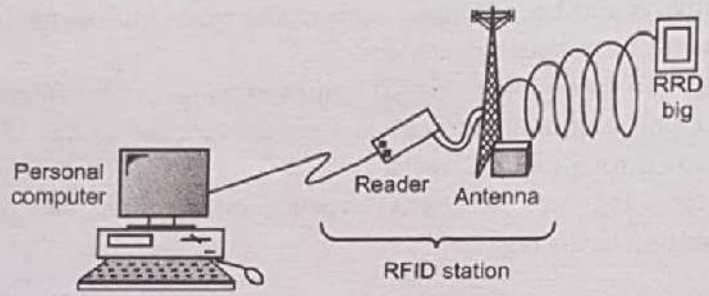


Fig. 2.10 : RFID

- The following are the RFID components

1. **Tags:**

- An RFID tag is an object that can be incorporated into a product, animal, or person for the purpose of identification using radio waves.
- There are two types of tags namely, Passive tags and Active tag. Passive tags tag require no internal power source, whereas active tags require a power source.

2. **Transponder:**

- The transponder emits messages with an identification number that is retrieved from a database and acted upon accordingly.
- The writable memory is used to transmit information among RFID readers in different locations.

3. **The Interrogator:**

- An antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it.
- When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal.

4. **Reader :**

- The reader decodes the data encoded in the tag circuit and the data is passed to the host computer.
- The application software on the host processes the data.

2.3.2.2 Risks and Benefits of Applying RFID in the Manufacturing Sector

- Radio Frequency Identification (RFID), in particular passive RFID, has become increasingly common in industrial environments as a way to track and trace products, assets, and material flow.

- Although the technology has been around for decades, recent advances in tag design have driven the cost down to levels that are helping fuel its acceptance in a wide variety of industries.
- RFID interrogators, which capture and transfer information to and from tags (transponders) via radio waves, are ideal for the most challenging industrial environments.
- RFID, in contrast to traditional vision-based bar code reading systems, doesn't require a direct line of sight to object identifiers.
- As a result, High Frequency (HF) and Ultra High Frequency (UHF) RFID systems have made it possible to track a wide range of products through the entire supply chain with more accuracy and timeliness. .
- Yet, despite the advantages, many industrial facilities are still hesitant to incorporate RFID into their mix of automation solutions.

1. **Improve the quality and transparency of data across the supply chain**

- Accurate data that is easily accessed makes it possible to solve a multitude of process inefficiencies. The best way to implement a system that results in the highest reliability and availability is by using the concept of 'distributed data."
- In this context, distributed data refers to live data that is attached directly to the object and can be modified automatically at process checkpoints.
- When data is read from a tag, answers are provided to the questions: What? Why? Where? and When? This is the very essence of RFID applications in industry.

2. **Make it easier to implement flexible manufacturing processes**

- Staying competitive often means producing more from the same production line. In order to make production processes more flexible, there must also be flexibility in the content and delivery of data to the various manufacturing cells.
- The ability to accommodate and respond to a higher influx of constantly changing data is necessary. RFID is used to reliably read and write data directly to a tag on an object in real-time. This capability can be leveraged to make flexible manufacturing a reality.

3. **Increase the accuracy of and reduce the time spent taking inventories**

- Manually counting inventory is an extremely tedious; time consuming, inefficient, and inaccurate method.
- RFID can be used to reduce or eliminate the need for "hand-scanning,' resulting in immediate and significant improvements in inventory tracking. These results directly impact the customer experience and lead to increased sales.

4. **Reliable track and trace in challenging physical environments**

- Since RFID does away with the requirement that there be a direct line of sight to the object's identifier, standard barcode labels (that can be ruined by extreme environmental conditions) can be replaced with encapsulated RFID tags.
- The need for reading and/or writing data to an object, when process conditions are extreme, can be handled by attaching these durable RFID tags.
- Conditions such as high humidity, drastic temperature swings, exposure to chemicals and paints, extremely high temperatures, rough handling, and dirt wreak havoc on conventional paper barcode labels.
- Specially encapsulated RFID tags are designed to survive and perform reliably in even the most challenging of environments.

5. **Increase efficiency and cut down on rework**

- RFID can be particularly advantageous in closed loop systems where reusable transport mechanisms are used.

- Real-time visibility allows the observation and close monitoring of products and processes so that quick action can be taken and process improvements that have a major impact on quality can be made in a timely manner with laser point precision.

2.3.2.3 Advantages of RFID

1. The RFID systems need low maintenance cost.
2. As line of sight communications is not needed the RFID tags can be read/written in dirty conditions also.
3. They can handle large amount of data.
4. RFID is not affected by objects like paper, plastic, clothing, non- metallic materials that placed between the antenna and RFID tag.
5. It provides secure and reliable data.
6. RFID supports multiple tag reads in shark interval of time.
7. Every RFID device has a unique serial number used for identification.
8. The detection process is automatic.

2.3.2.4 Disadvantages of RFID

1. RFID deals with assembly and inserting a computerized chip (RFID tag) in the device.
2. If RFID tags are installed in the metal and liquid products, it becomes tedious for the reader to read the data. The liquid and metal surface reflect two radio waves, this makes two RFID tags unreadable.
3. The life of active RFID's is battery dependent.
4. RFID systems are susceptible to virus.

2.4 BLUETOOTH TECHNOLOGY, Wi-Max AND Wi-Fi

2.4.1 Bluetooth Technology

- Bluetooth is a wireless personal area network (WPAN) technology. It is based on IEEE 802.15.1 standards.
- Bluetooth provides short-range, low-cost connectivity between portable devices. Bluetooth is limited in range (<10 meters) and provides speeds of about 780 kbps. Thus, Bluetooth is used as a replacement for cables and wired networks to form small Ad hoc private wireless LANs.

Definition of the Terms Used in Bluetooth:

1. **Piconet:**

- A collection of devices connected via Bluetooth technology in an ad hoc fashion.
- A piconet starts with two connected devices, such as a PC and cellular phone, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations.
- However, when establishing a piconet, one unit will act as a master for synchronization purposes, and the other(s) as slave(s) for the duration of the piconet connection.

2. **Scatternet:**

- Two or more independent and non-synchronized piconets that communicate with each other.
- A slave as well as a master unit in one piconet can establish this connection by becoming a slave in other piconet.

3. **Master Unit:**

- The device in the piconet whose clock and hopping sequence are used to synchronize all other devices in the piconet.

4. **Slave Units:**

- All devices in a piconet that are not the master (up to seven active units for each master).

5. **MAC Address:**

- A 3-bit medium access control address used to distinguish between units participating in the piconet.

6. **Parked Units:**

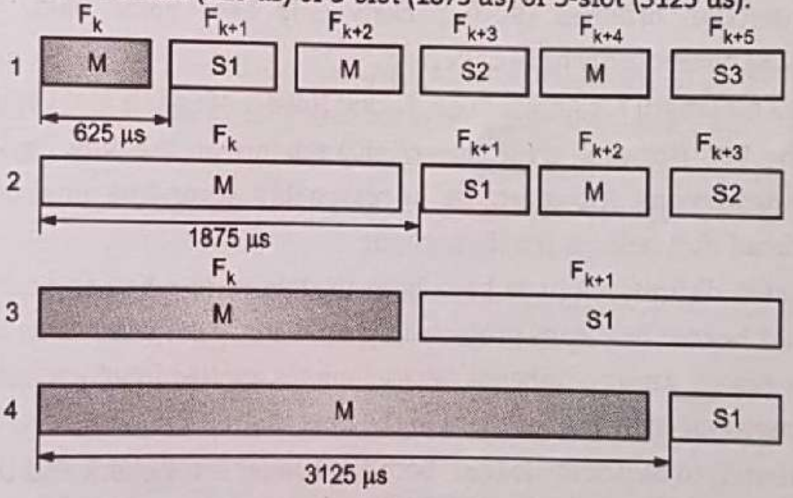
- Devices in a piconet which are time-synchronized but do not have MAC addresses.

7. **Sniff and Hold Mode:**

- Devices that are synchronized to a piconet, and which have temporarily entered power-saving mode in which device activity is reduced.

2.4.1.1 Frame Format in Bluetooth Technology

- Bluetooth packet can be of 1-slot (625 us) or 3-slot (1875 us) or 5-slot (3125 us).



1. One-slot symmetrical, 3. Three-slot symmetrical,
2. Three-slot asymmetrical,4. Five-solt asymmetrical

Fig. 2.11 (a): Bluetooth Packets

- Each packet consists of a 72 bit access code. The access code is used for packet identification. Every packet exchanged on the channel is preceded by its access code.
- Recipients on the piconet compare incoming signals with access code. If the two do not match, the received packet is not considered valid and rest of its contents are ignored.
- The 72 bit access code is derived from master identity.Thus, access code is also used for synchronization and compensating for offset. The access code is robust and resistant to interference.

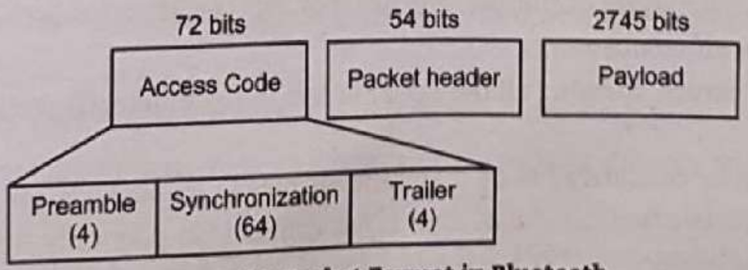


Fig. 2.11 (b): Packet Format in Bluetooth

- Header part of the packet is used by the Link Control (LC) logical channel. It has the following format:

LSB 3	4	1	1	1	8 MSB
AM_ADDR	TYPE	FLOW	ARQN	SEQN	HEC

Fig. 2.12 : Header format

- **AM_ADDR:** Temporary address assigned to active members of the piconet, used on all packets in both directions sent between the master and the addressed slave. An all-zero AM_ADDR is used to broadcast to all slaves.
- **TYPE:** Type of packet. There are 12 types of packets for each SCO and ACL physical links, and four types of common control packets for both.
- **FLOW:** For flow control.
- **ARQN:** For ACK.
- **SEQN:** Contains sequence number for packet ordering.
- **HEC:** Header error check for header integrity.

There can be two types of payload:

1. Voice and 2. Data.

- Synchronous connection oriented (SCO) packets only have voice field, while Asynchronous connection less (ACL) packets only have data field.
- Packet consist of 72 bit length for Access Code, Packet Header of 54 bits and Payload of 2745 bits.
- The purpose of the FEC (forward error correction) scheme on the data payload is to reduce the number of retransmissions. However, in a reasonably error-free environment, FEC creates unnecessary overhead that reduces the throughput.
- Therefore, the packet definitions have been kept flexible as to whether or not to use FEC in the payload. The packet header is always protected by a 1/3 rate FEC. It contains link information and should survive bit errors. An unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot.
- For a data transmission to be acknowledged, both the header error check and the cyclic redundancy check must be satisfied, otherwise a negative acknowledgment is returned. (See Fig. 2.9)

Three error correction schemes are defined for the Bluetooth baseband controller:

1. 1/3 rate forward error correction (FEC) code.
2. 2/3 rate forward error correction code.
3. Automatic repeat request (ARQ) scheme for data.

2.4.1.2 Bluetooth Architecture

- Bluetooth is both a hardware-based radio system and a software stack that specifies the linkages between the architecture layers of the two. The heart of this specification is the protocol stack, which is used to define how Bluetooth works.
- The Bluetooth architecture, showing all the major layers in the Bluetooth system, are depicted in the Fig. 2.13.
- The layers below can be considered to be different hurdles in an obstacle course. This is because all the layers function one after the other. One layer comes into play only after the data has been through the previous layer.

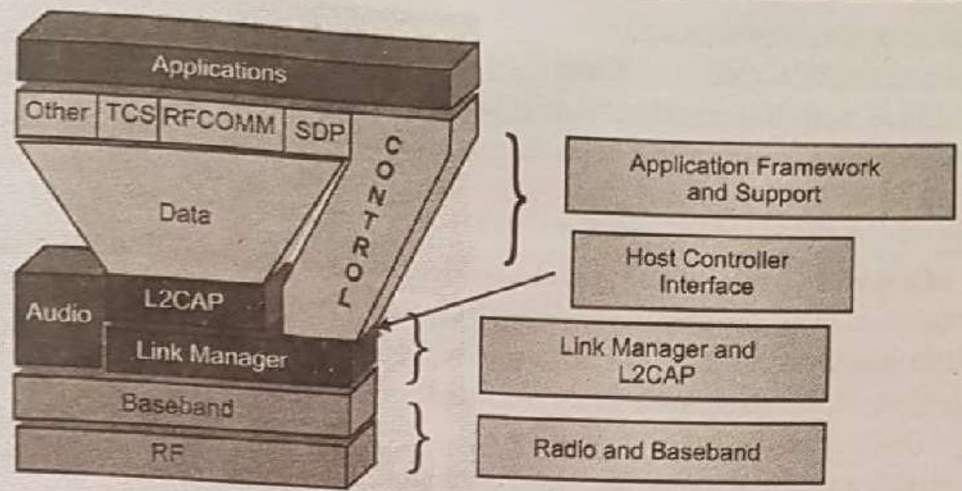


Fig. 2.13: Bluetooth Architecture

Bluetooth Main Groups:

1. **Radio:** The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.
2. **Baseband:** The Baseband layer describes the specification of the Bluetooth Link Controller (LC), which carries out the baseband protocols and other low-level link routines. It specifies Piconet/Channel definition, "Low-level" packet definition, Channel sharing
3. **LMP:** The Link Manager Protocol (LMP) is used by the Link Managers (on either side) for link set-up and control.
4. **HCI:** The Host Controller Interface (HCI) provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.
5. **L2CAP:** Logical Link Control and Adaptation Protocol (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.
6. **RFCOMM:** The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10.
7. **SDP:** The Service Discovery Protocol (SDP) provides a means for applications to discover, which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services.

2.4.2 Wi-Max

- The 'World Interoperability for MicroAcess, Inc. (WiMAX)' forum, an industry group, focuses on creating advanced technology solution for high speed wide area internet access.
- The WiMAX product certification program ensures interoperability between WiMAX equipment from vendors worldwide.
- WiMAX can serve as a backbone for 802.11 hotspots for connecting to the internet. Alternatively, users can connect mobile devices such as laptops and handsets directly to WiMAX base stations. Mobile devices connected directly can achieve a range of 4 to 6 miles.
- There are 2 types of WiMAX, fixed WiMAX (IEEE 802.16d-2004) and mobile WiMAX (IEEE802.16e-2005). Fixed WiMAX is a point-to-multipoint technology, whereas mobile WiMAX is a multipoint-to-multipoint technology, similar to that of a cellular infrastructure.

Salient Features Supported by WiMAX:

1. **High Data Rates:** WiMAX can typically support data rates from 500 Kbps to 2 Mbps. The inclusion of multi-input multi-output(MIMO) antenna techniques along with flexible sub-channelization schemes, advanced coding and modulation all enable mobile to support peak downlink data rates of 63 Mbps per sector and peak uplink data rates of up to 28 Mbps per sector in a 10 MHz channel.
2. **Quality of Service (QoS):** WiMAX has clearly defined QoS classes for applications with different requirements such as VoIP, real time videostreaming, file transfer and web traffic.
3. **Scalability:** Mobile WiMAX is designed to able to work in different channelization from 1.25 to 20 MHz to comply with varied world-wide requirements.
4. **Security:** There is support for diverse set of user credentials like SIM/USIM cards, smart cards, digital certificates, username/password schemes. All this is based on relevant 'extensible authentication protocol (EAP)' methods for credential type.
5. **Mobility:** Mobile WiMAX supports optimized handoff schemes with latencies less than 50ms to ensure that real time applications such as VoIP can be performed without service degradation. Flexible key management schemes assume that security is maintained during handoff.

WiMAX Physical Layer (PHY):

- For bands in 10-66GHz range, 802.16 defines one interface called Wireless MAN-SC.
- For 2-11GHz (both licensed and unlicensed):
  - ➢ Wireless MAN-SC (single carrier modulation)
  - ➢ Wireless MAN-OFDM (256 carrier OFDM with access to different stations using TDMA)
  - ➢ Wireless MAN-OFDM (2048 carrier OFDM by assigning subset of carriers to individual station)
- WiMAX PHY features include 'Adaptive Modulation and Coding (AMC)', 'Hybrid Automatic Repeat Request (HARQ)', 'Channel Quality Indicator Channel (CQICH)' which is a feedback channel.
- All these features provide robust link adoption in mobile environment at vehicular speeds in excess of 120Km/h.

WiMAX Medium Access Control (MAC):

- Each subscriber station need to compete for media only one (for entry). Then, WiMAX base station provides time slot to each subscriber station which may increase or decrease depending on need.
- There is a scheduling algorithm for service to each station. This algorithm is robust and not affected by over loading and over subscription.
- WiMAX supports different transport technologies such as IPv4, IPv6 and Ethernet.
- WiMAX mesh networking allows subscriber stations to communicate with each other i.e. "Subscriber" mode and with base station i.e. "base station" mode simultaneously.

Spectrum Allocation for WiMAX:

- The biggest spectrum segment for WiMAX is around 2.5GHz.
- The other bands are around 3.5HZ, 2.3/2.5GHz, or 5GHz, with 2.3/2.5GHz.

Other Features:

- The mesh mode of WiMAX enables subscriber stations to relay traffic to one another. Thus, a station that does not have line-of-sight with the base station can get its traffic from another station.
- WiMAX technology can provide fast and cheap broadband access to markets that lack infrastructure (fiber optics, copper wire), such as rural areas and unwired countries. WiMAX can also be used in backup during disasters, which may lead the wired networks to get broken down.
- As mobile WiMAX is scalable in both radio access and network architecture, it provides flexibility in network deployment options and service offerings.

- Mobile WiMAX based on 802.16e uses OFDMA in which carriers are divided among users to form sub channels. The coding and modulation are adapted separately for each sub channel.
- SOFDMA is an enhancement of OFDMA that scale the number of subcarriers in a channel with possible values of 128, 512, 1024, and 2048.
- 802.16e includes power-saving and sleep modes to extend battery life if mobile devices.
- 802.16e also supports hard and soft handoff to provide users with seamless connections as they move across coverage areas of adjacent cells.

Difference between Wi-Fi and WiMAX:

Table 2.4

Sr. No	Wi-Fi	WiMAX
1.	Wi-Fi technology is based on IEEE 802.11 standards.	WiMAX technology is based on IEEE 802.16 standards.
2.	802.11a-OFDM,maximum rate=54Mbps.,802.11b-DSSS,maximum rate=11Mbps.,802.11g-OFDM,maximum rate=54Mbps.	802.16-OFDM, maximum rate = 50Mbps., 802.16e-OFDM, maximum rate~30Mbps.
3.	The stations gain access to media based on CSMA/CA and back off algorithm schemes.	There is time slot for each station and there is scheduling algorithm used by base station.
4.	Range is less than 100 meters.	A kilometer non-line-of-sight, more with line-of-sight.
5.	Indoor Environment.	Outdoor Environment.
6.	No Quality of Service.	Five Quality of service enforced by base station.

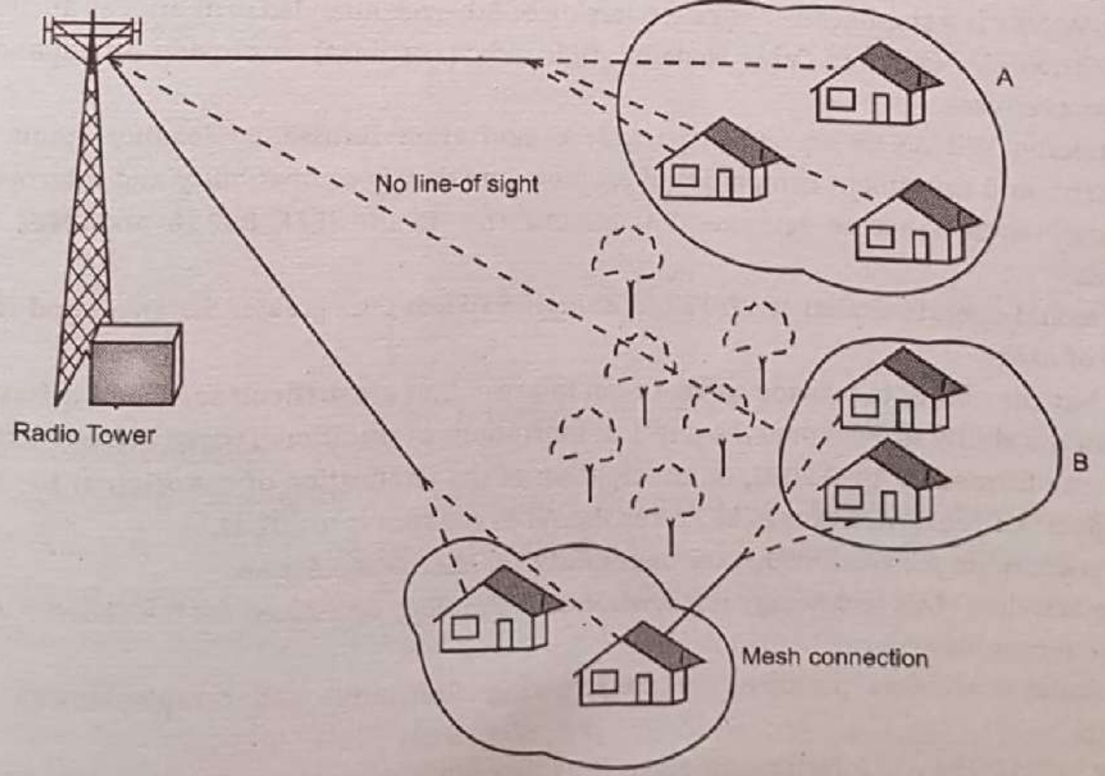


Fig. 2.14 : Mesh mode in IEEE 802.16(WiMAX)

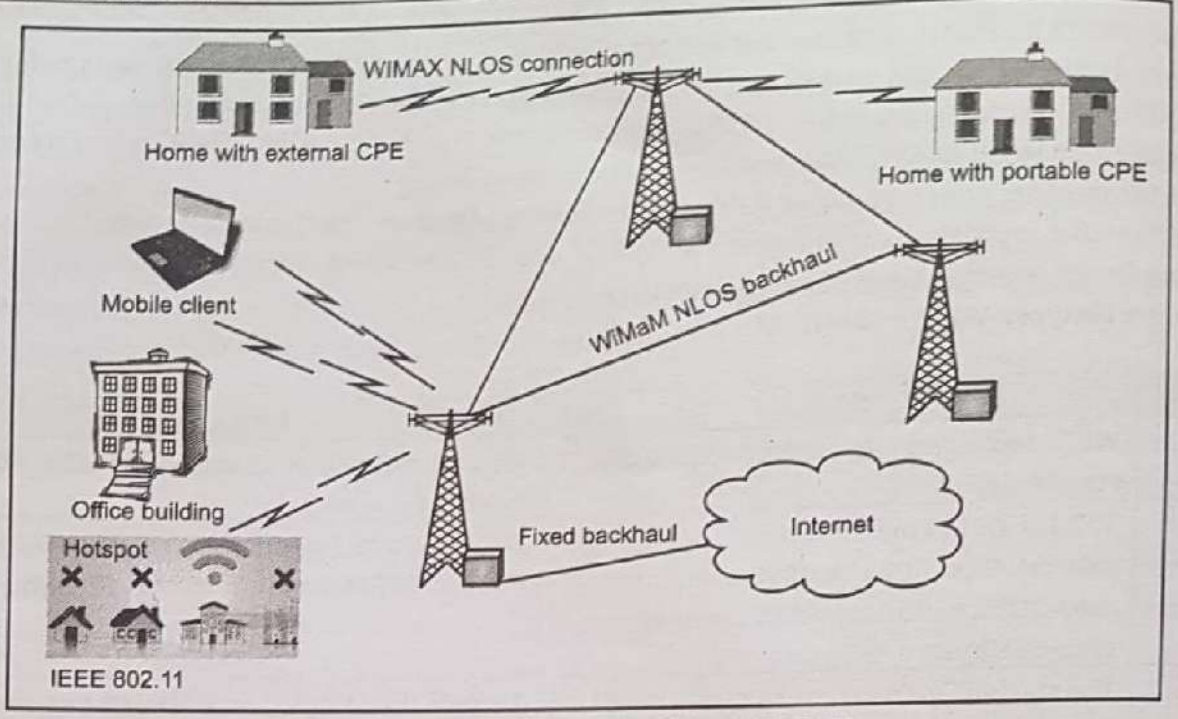


Fig. 2.15 : Applications of IEEE 802.16 (WiMAX)

2.4.2.1 Different Standards of WiMax

- WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.
- Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.
- More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards.
- WiMAX would operate similar to Wi-Fi, but at higher speeds over greater distances and for a greater number of users.
- WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure.
- WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the Wi-Fi Alliance is to 802.11.
- WiMAX is acronym for Worldwide Interoperability for Microwave Access.
- Based on Wireless MAN technology it is a wireless technology optimized for the delivery of IP centric services over a wide area.
- It is a scalable wireless platform for constructing alternative and complementary broadband networks.
- The IEEE 802.16, the Air Interface for Fixed Broadband Wireless Access Systems, also known as the IEEE Wireless MAN air interface, is an emerging suite of standards for fixed, portable and mobile BWA in MAN.

Table 2.5

	802.16	802.16a	802.16e
Spectrum	10-66 GHz	2-11 GHz	< 6 GHz
Configuration	Line of slight	Non-line of slight	Non-line of slight
Bit Rate	32 to 134 Mbps (28 MHz channel)	≤70 or 100 Mbps (20 MHz Channel)	Up to 15 Mbps
Modulation	QPSK, 16-QAM, 64-QAM	256 sub-carrier OFDM using QPSK, 16-QAM, 256-QAM.	Same as 802.16a
Mobility	Fixed	Fixed	≤75 MPH
Channel Bandwidth	20, 25, 28 MHz	Selectable 1.25 to 20 MHz	5 MHz (Planned)
Typical cell radius	1-3 miles	3-5 miles	1-3 miles
Completed	Dec, 2001	Jan 2003	2nd half of 2005

IEEE 802.16a:

- WiMAX is such an easy term that people tend to use it for the 802.16 standards and technology themselves, although strictly it applies only to systems that meet specific conformance criteria laid down by the WiMAX Forum.
- The 802.16a standard for 2-11 GHz is a wireless Metropolitan Area Network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.
- It can be used to connect 802.11 hot spots to the Internet, provide campus connectivity, and provide a wireless alternative to cable and DSL for last mile broadband access.

IEEE 802.16:

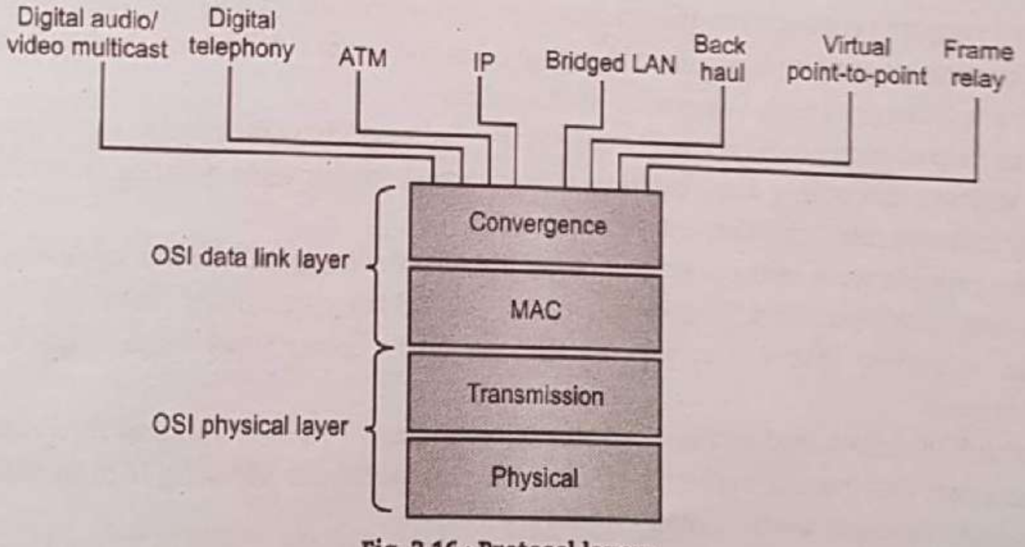


Fig. 2.16 : Protocol layers

There are Four Protocol Layers:

1. **Physical Layer :** It is responsible for performing functions like encoding/decoding of signals, generating preamble, transmitting/receiving a data bit. It comprises of the frequency band and medium of transmission.
2. **Transmission Layer:** It deals with encoding/decoding signals, generating preamble, transmitting / receiving data bits.
3. **Medium Access Control Layer (MAC) Layer:** It is responsible for transmitting the data frames and controlling wireless access. This layer is simple. It indicates when a subscriber or base station can begin transmission.
4. **Convergence Layer:** It provides functions that are required for providing a particular service.

Speed and Range:

- WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.
- WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet.
- WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.
- With WiMAX, users could really cut free from today's Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a Metro Zone.

WiMAX could potentially be deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz.

2.4.2.2 Advantages of WiMAX

- WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, Wi-Fi, and cellular backhaul, providing last-100 meter access from fiber to the curb and giving service providers another cost-effective option for supporting broadband services.
- WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.
- WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.
- WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive Voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications.
- WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.
- Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

2.4.2.3 Wi-MAX Technology

- WiMax stands for World Interoperability for Micro-wave Access. WiMAX is optimized for IP-based high-speed wireless broadband which will provide for a better mobile wireless broadband internet experience.

Features of WI-MAX Technology :

1. Wi MAX can typically support data rates from 500 kbps to 2 Mbps.
2. WiMAX also has clearly defined QoS classes for applications with different requirements such as VoIP, real-time video streaming, file transfer, and web traffic.

3. A cellular architecture similar to that of mobile phone systems can be used with a central base station controlling downlink/uplink traffic.
4. WiMAX is a family of technologies based on IEEE 802.16 standards.
5. Two main types of WiMAX, fixed WiMAX (point-to- multipoint Technology) and mobile WiMAX (multipoint-to-multipoint technology).
6. WiMAX uses orthogonal frequency division multiple access (OFDMA) technology which has inherent advantages in, spectral efficiency, advanced antenna performance, and improved multipath performance.
7. Mobile devices connected directly can achieve a range of 4 to 6 miles.
8. Frequency band -2 to 11 GHz (unlicensed).
9. channel bandwidth: 1.25 MHz to 20 MHz.

Advantages:

1. Single station can serve hundreds of users.
2. Speed of 10 Mbps at 10 kilometers with line-of-sight.

Disadvantages:

1. Line of sight is needed for longer connection.
2. Weather conditions like rain can interrupt the signal.
3. Other wireless equipment's can interrupt the signal.
4. Multiplied frequencies are used.

Applications:

1. T1 level service for enterprise.
2. DSL level service for SOHO.
3. Wireless backhaul for hotspots.
4. Coverage is 50 km.
5. Modulation.
6. Uplink S OFDMA.
7. Downlink S OFDMA.
8. Channel bandwidth 40MHz.
9. Speed – 120 Km/hr.
10. Compliance – non compliant with 2G and 3G.

2.4.3 Wi-Fi

- WiFi stands for Wireless Fidelity. WiFiIt is based on the IEEE 802.11 family of standards and is primarily a Local Area Networking (LAN) technology designed to provide in-building broadband coverage.
- Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.
- WiFi has become the *de facto* standard for *last mile* broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point.
- WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but WiFi systems are not designed to support high-speed mobility.

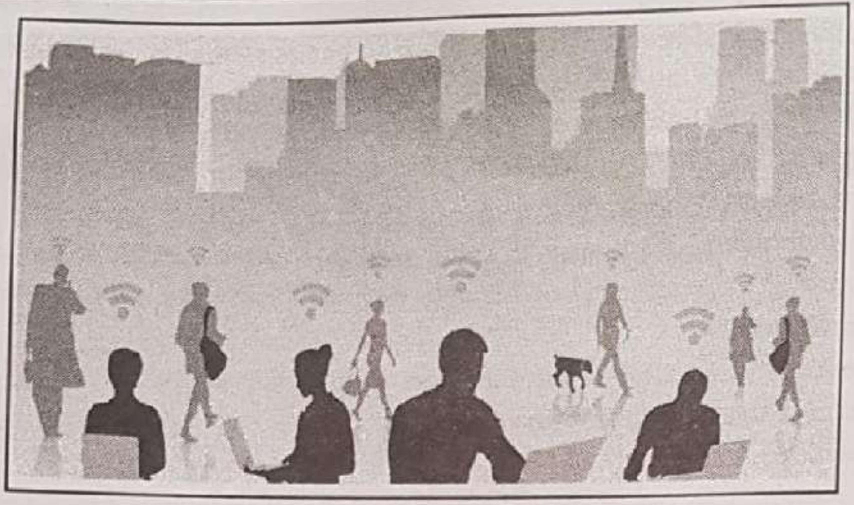


Fig. 2.17 : Wi-Fi Technology

- One significant advantage of WiFi over WiMAX and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also being built into a variety of devices, including Personal Data Assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

WiFi is Half Duplex:

- All WiFi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all WiFi networks are half duplex.
- There are equipment vendors who market WiFi mesh configurations, but those implementations incorporate technologies that are not defined in the standards.

Channel Bandwidth:

- The WiFi standards define a fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g networks.

2.4.3.1 Wi-Fi - Working Concepts

Radio Signals:

- Radio Signals are the keys, which make WiFi networking possible. These radio signals transmitted from WiFi antennas are picked up by WiFi receivers, such as computers and cell phones that are equipped with WiFi cards.
- Whenever, a computer receives any of the signals within the range of a WiFi network, which is usually 300 — 500 feet for antennas, the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.
- Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

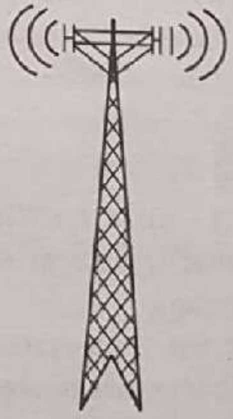


Fig. 2.18 : Wi-Fi concept

WiFi Cards:

- WiFi cards are invisible cords that connect your computer to the antenna for a direct connection to the internet.

- WiFi cards can be external or internal. If a WiFi card is not installed in your computer, then you may purchase a USB antenna attachment and have it externally connect to your USB port, or have an antenna-equipped expansion card installed directly to the computer (as shown in the Fig. 2.19).
- For laptops, this card will be a PCMCIA card which you insert to the PCMCIA slot on the laptop.

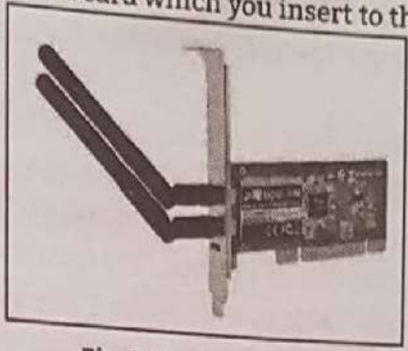


Fig. 2.19 : Wi-Fi cards

2.4.3.2 WiFi Hotspots

- A WiFi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a WiFi enabled device such as a Pocket PC encounters a hotspot, the device can then connect to that network wirelessly.
- Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide.
- The 802.11g standard is backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter.
- The largest public WiFi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.

Fig. 2.20 : Wi-Fi Hotspot

- Hotspots are increasingly developing around the world. In fact, T-Mobile USA controls more than 4,100 hotspots located in public locations such as Starbucks, Borders, Kinko's, and the airline clubs of Delta, United, and US Airways. Even select McDonald's restaurants now feature WiFi hotspot access.
- Any notebook computer with integrated wireless, a wireless adapter attached to the motherboard by the manufacturer, or a wireless adapter such as a PCMCIA card can access a wireless network.

Furthermore, all Pocket PCs or Palm units with Compact Flash, SD I/O support, or built-in WiFi, can access hotspots.

- Some Hotspots require WEP key to connect, which is considered as private and secure. As for open connections, anyone with a WiFi card can have access to that hotspot. So in order to have internet access under WEP, the user must input the WEP key code.

2.4.3.3 WiFi IEEE Standards

- The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.
- There are several specifications in the 802.11 family –
  1. **802.11 :** This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS).
  2. **802.11a :** This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
  3. **802.11b :** The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
  4. **802.11g :** This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.
- Here is the technical comparison between the three major WiFi standards.

Table 2.6

Feature	WiFi (802.11b)	WiFi (802.11a/g)
Primary Application	Wireless LAN	Wireless LAN
Frequency Band	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	25 MHz	20 MHz
Half/Full Duplex	Half	Half
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth	<=0.44 bps/Hz	≤=2.7 bps/Hz
Efficiency	?	?
Modulation	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	None	Convolutional Code
Encryption	Optional- RC4m (AES in 802.11i)	Optional- RC4(AES in 802.11i)
Mobility	In development	In development
Mesh	Vendor Proprietary	Vendor Proprietary
Access Protocol	CSMA/CA	CSMA/CA

2.4.3.4 Wi-Fi – Access Protocols

- IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

- WiFi systems are the half duplex shared media configurations, where all stations transmit and receive on the same radio channel.
- The fundamental problem of a radio system is that a station cannot hear while it is sending, and hence it is impossible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the Distributed

Distributed Control Function (DCF)

- According to DCF, a WiFi station will transmit only when the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.
- The incidence of collisions will increase as the traffic increases or in situations where mobile stations cannot hear each other.

2.4.3.5 Wi-Fi - Quality of Service (QoS)

- There are plans to incorporate quality of service (QoS) capabilities in WiFi technology with the adoption of the IEEE 802.11e standard.
- The 802.11e standard will include two operating modes, either of which can be used to improve service for voice:
  1. WiFi Multimedia Extensions (WME) – Mandatory
  2. WiFi Scheduled Multimedia (WSM) – Optional
  3. WiFi Multimedia Extensions (WME)
- WiFi Multimedia Extensions use a protocol called Enhanced Multimedia Distributed Control Access (EDCA), which is an extension of an enhanced version of the Distributed Control Function (DCF) defined in the original 802.11 MAC
- The enhanced part is that EDCA will define eight levels of access priority to the shared wireless channel.
- Like the original DCF, the EDCA access is a contention-based protocol that employs a set of waiting intervals and back-off timers designed to avoid collisions.
- However, with DCF all stations use the same values and hence have the same priority for transmitting on the channel.
- With EDCA, each of the different access priorities is assigned a different range of waiting intervals and back-off counters.
- Transmissions with higher access priority are assigned shorter intervals. The standard also includes a packet-bursting mode that allows an access point or a mobile station to reserve the channel and send 3- to 5-packets in a sequence.

WiFi Scheduled Multimedia (WSM):

- True consistent delay services can be provided with the optional WiFi Scheduled Multimedia (WSM). WSM operates like the little used Point Control Function (PCF) defined with the original 802.11 MAC.
- In WSM, the access point periodically broadcasts a control message that forces all stations to treat the channel as busy and not attempt to transmit. During that period, the access point polls each station that is defined for time sensitive service.
- To use the WSM option, devices need to send a traffic profile describing bandwidth, latency, and jitter requirements. If the access point does not have sufficient resources to meet the traffic profile, it will return a *busy signal*.

2.4.3.6 Wi-Fi Security

- Security has been one of the major deficiencies in WiFi, though better encryption systems are now becoming available. Encryption is optional in WiFi, and two different techniques have been defined.
- These techniques are given here –

1. **Wired Equivalent Privacy (WEP)**

- An RC4-based 40-or 104-bit encryption with a static key. WiFi Protected Access (WPA).
- This is a new standard from the WiFi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet. That changing key functionality is called the Temporal Key Integrity Protocol (TKIP).

2. **IEEE 802.11i/WPA2**

- The IEEE is finalized the 802.11i standard, which is based on a far more robust encryption technique called the Advanced Encryption Standard.
- The WiFi Alliance designate products that comply with the 802.11i standard as WPA2. However, implementing 802.11i requires a hardware upgrade.

2.4.3.7 Wi-Fi Network Services

- The picture has become somewhat confused as service providers started using WiFi to deliver services for which it was not originally designed.
- The two major examples of this are Wireless ISPs and City-wide WiFi mesh networks.

1. **Wireless ISPs (WISPs)**

- One business that grew out of WiFi was the Wireless ISP (WISP). This is an idea of selling an Internet access service using wireless LAN technology and a shared Internet connection in a public location designated as a hot spot.
- From a technical standpoint, access to the service is limited based on the transmission range of the WLAN technology. You have to be in the hotspot (i.e. within 100m of the access point) to use it.
- From a business standpoint, users either subscribe to a particular carrier's service for a monthly fee or access the service on a demand basis at a fee per hour.
- While the monthly fee basis is most cost effective, there are few inter carrier access arrangements, so you have to be in a hotspot operated by your carrier in order to access your service.

2. **City-Wide Mesh Networks**

- To address the limited range, vendors like Mesh Networks and Tropos Networks have developed mesh network capabilities using WiFi's radio technology.
- The idea of a radio mesh network is that messages can be relayed through a number of access points to a central network control station. These networks can typically support mobility as connections are handed off from access point to access point as the mobile station moves.
- Some municipalities are using WiFi mesh networks to support public safety applications (i.e. terminals in police cruisers) and to provide Internet access to the community (i.e. the city-wide hot spot).

Wi-Fi - Radio Modulation

- WiFi systems use two primary radio transmission techniques.

1. **802.11b (<=11 Mbps) :** The 802.11b radio link uses a direct sequence spread spectrum technique called complementary coded keying (CCK). The bit stream is processed with a special coding and then modulated using Quadrature Phase Shift Keying (QPSK).

2. **802.11a and g (<=54 Mbps) :** The 802.11a and g systems use 64-channel Orthogonal Frequency Division Multiplexing (OFDM). In an OFDM modulation system, the available radio band is divided into a number of sub-channels and some of the bits are sent on each. The transmitter encodes the bit streams on the 64 subcarriers using Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), or one of two levels of Quadrature Amplitude Modulation (16, or 64-QAM). Some of the transmitted information is redundant, so the receiver does not have to receive all of the sub-carriers to reconstruct the information.

- The original 802.11 specifications also included an option for frequency hopping spread spectrum (FHSS), but that has largely been abandoned.

Adaptive Modulation:

1. WiFi uses adaptive modulation and varying levels of forward error correction to optimize transmission rate and error performance.
2. As a radio signal loses power or encounters interference, the error rate will increase. Adaptive modulation means that the transmitter will automatically shift to a more robust, though less efficient, modulation technique in those adverse conditions.

2.4.3.8 Wi-Fi Major Issues

- There are a few issues that are assumed to be the cause behind the sluggish adoption of WiFi technology:
  1. **Security Problems:** Security concerns have held back WiFi adoption in the corporate world. Hackers and security consultants have demonstrated how easy it can be to crack current security technology known as wired equivalent privacy (WEP) used in most WiFi connections. A hacker can break into a WiFi network using readily available materials and software.
  2. **Compatibility and Interoperability:** One of the major problems with WiFi is its compatibility and interoperability. For example, 802.11a products are not compatible with 802.11b products. Due to different operating frequencies, 802.11a hotspots would not help an 802.11b client. Due to lack of standardization, harmonization, and certification, different vendors come out with products that do not work with each other.
  3. **Billing Issues:** WiFi vendors are also looking for ways to solve the problem of back-end integration and billing, which have dogged the roll-out of commercial WiFi hotspots. Some of the ideas under consideration for WiFi billing such as per day, per hour, and unlimited monthly connection fees.
  4. **Wi-Fi Summary:** WiFi is a universal wireless networking technology that utilizes radio frequencies to transfer data. WiFi allows high-speed Internet connections without the use of cables. The term WiFi is a contraction of "wireless fidelity" and commonly used to refer to wireless networking technology. The WiFi Alliance claims rights in its uses as a certification mark for equipment certified to 802.11x standards.
  5. **WiFi is a Freedom:** Freedom from wires. It allows you to connect to the Internet from just about anywhere - a coffee shop, a hotel room, or a conference room at work. It is almost 10 times faster than a regular dial-up connection. WiFi networks operate in the unlicensed 2.4 radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, respectively.
  6. To access WiFi, we need WiFi enabled devices (laptops or PDAs). These devices can send and receive data wirelessly in any location equipped with WiFi access.

2.5 MOBILE IP

- Mobile IP is a proposed standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP.
- Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks.
- Mobile IP is scalable for the Internet because it is based on IP—any media that can support IP can support Mobile IP.

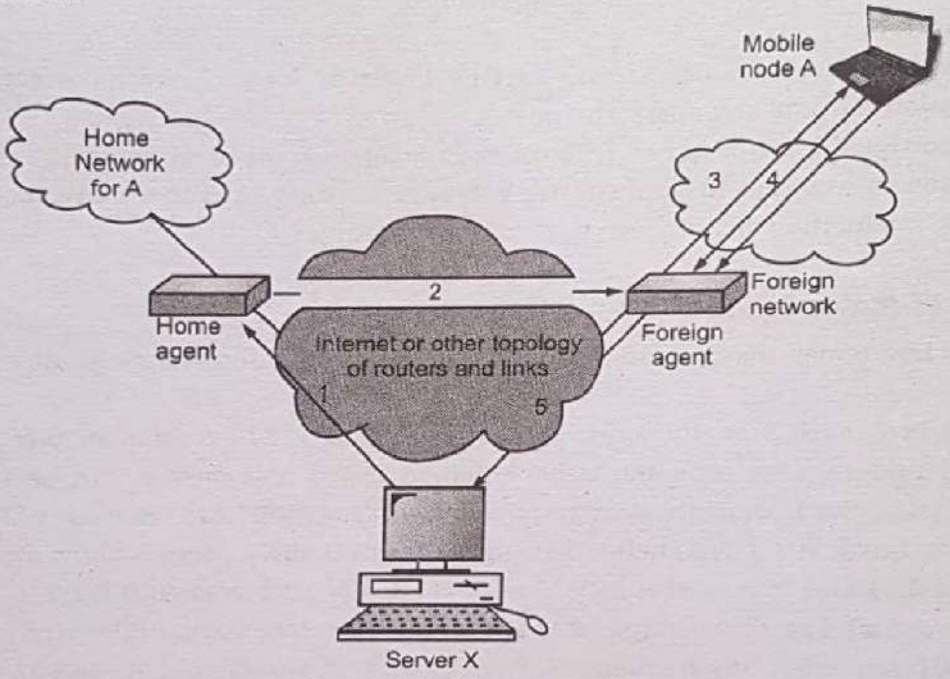


Fig. 2.21 : Mobile IP Scenario

- Mobile IP is designed to support host mobility on the internet. User is connected to one or more applications across the internet, the user's point of attachment changes dynamically and that all connections are automatically maintained despite the change.
- Server X transmits an IP datagram for mobile nodes A with A's address in IP header. IP datagram is routed to A's home network.
- At home N/w the incoming IP datagram is intercepted by home agent. The home agent encapsulates the entire datagram inside a new IP datagram. The use of an outer IP datagram with a different destination IP address is known as "tunneling". This IP datagram is routed to foreign agent.
- Foreign agent strips off the outer IP header, encapsulates the original IP datagram in a N/w level Packet Data Unit (PDU) and delivers the original datagram to A across the foreign network.
- When A sends the IP datagram to X, it uses X's IP address. This is a fixed address that is X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network to X. This router is also a foreign agent.
- The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

1. Mobile IP Capabilities
2. Registration
3. Discovery
4. Tunneling

2.5.1 Agent Advertisement Packet including Mobility Extension

- Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network.
- An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.
- Agent Discovery is the method by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another.
- When connected to a foreign network, the methods specified in this section also allow the mobile node to determine the foreign agent care-of address being offered by each foreign agent on that network.
- Mobile IP extends ICMP Router Discovery as its primary mechanism for Agent Discovery. An Agent Advertisement is formed by including a Mobility Agent Advertisement Extension in an ICMP Router Advertisement message.

Agent Discovery:

- A mobile node has to find a foreign agent when it moves away from its home network. To solve this problem, mobile IP describes two methods namely, agent advertisement and agent solicitation.

1. **Agent Advertisement:**

- For this method, foreign agents and home agents advertise their presence periodically using special agent advertisement messages, which are broadcast into the subnet.
- Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message.
- The agent advertisement packet according to RFC 1256 with the extension for mobility is shown below.

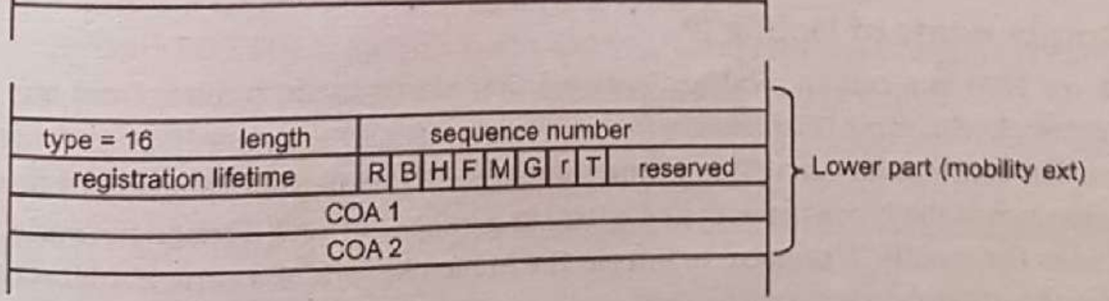


Fig. 2.22 : Agent advertisement packet

- The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them. The Type is set to 9, the code can be 0, if the agent also routes traffic from non-mobile nodes, or 16, if it does not route anything other than mobile traffic.
- The number of addresses advertised with this packet is in #addresses while the addresses themselves follow as shown.

- Lifetime denotes the length of time this advertisement is valid. Preference levels for each address help a node to choose the router that is the most eager one to get a new node.
- The extension for mobility has the following fields defined: type is set to 16, length depends on the number of COAs provided with the message and equals 6 + 4*(number of addresses).
- The sequence number shows the total number of advertisements sent since initialization by the agent. By the registration lifetime the agent can specify the maximum lifetime in seconds a node can request during registration.
- The following bits specify the **characteristics of an agent** in detail:
  - The R bit (registration) shows, if a registration with this agent is required even when using a co-located COA at the MN.
  - If the agent is currently too busy to accept new registrations it can set the B bit.
  - The following two bits denote if the agent offers services as a home agent (H) or foreign agent (F) on the link where the advertisement has been sent.
  - Bits M and G specify the method of encapsulation used for the tunnel. While IP-in-IP encapsulation is the mandatory standard.
  - M can specify minimal encapsulation and G generic routing encapsulation.
  - In the first version of mobile IP (RFC 2002) the V bit specified the use of header compression according to RFC 1144. Now the field r at the same bit position is set to zero and must be ignored.
  - The new field T indicates that reverse tunneling is supported by the FA. The following fields contain the COAs advertised. A foreign agent setting the F bit must advertise at least one COA.
  - A mobile node in a sub-net can now receive agent advertisements from either its home agent or a foreign agent. This is one way for the MN to discover its location.

2. **Agent Solicitation:**

- Every mobile node should implement agent solicitation. The mobile node uses the same procedures, defaults, and constants for agent solicitation, as specified for ICMP router solicitation messages.
- The rate at which a mobile node sends solicitations is limited by the mobile node. The mobile node can send three initial solicitations at a maximum rate of one per second while searching for an agent.
- After registering with an agent, the rate at which solicitations are sent is reduced, to limit the overhead on the local network.

2.5.2 Components of Mobile IP

- Mobile IP (or MIP) is a communications protocol that allows users to move from one network to another network with same IP address.
- It ensures that communication will continue without user's sessions or connections being dropped. When a user leaves the home network and enters in another network (foreign network), the foreign network uses the mobile IP protocol to inform the home network of a care-of address to which all packets for the user's device should be sent.
- Home Address is the permanent IP address assigned to the mobile node. Mobile node uses this address in its home address. Care-Of Address (COA) is the temporary address used by a mobile node while it is moving away from its home network.
- Mobile IP has the following three components namely, Mobile Node, Home Agent and Foreign Agent.
  1. **Mobile Node:** Any device those have roaming facility such as a cell phone, personal digital assistant, or laptop.

2. **Home Agent:** It is a router on the home network and working as communication point with the Mobile Node. It stores information about mobile nodes whose permanent home address is in the home agent's network. It tunnels data from a called a Correspondent Node, to the roaming Mobile Node.

3. **Foreign Agent:** It available in another network and stores information about mobile nodes visiting its network. The Foreign Agent is a router that advertises care-of addresses, which are used by mobile IP. It also delivers packets from the Home Agent to the Mobile Node while roaming in another network.

Practice Questions

1. Describe the GPRS architecture and protocols. How many of them already exist in GSM?
2. To accommodate GPRS, What modifications are made to BSS?
3. Which part of GPRS interface should be modified if ATM replaces frame relay?
4. Compare channel request procedure in GPRS with that in GSM.
5. Write short note on: GPRS for 2.5G GSM and IS-136.
6. Explain GPRS Services.
7. What are limitations and applications of GPRS.
8. Write short note on GPRS-Quality of service.
9. Explain data packet routing and mobility management in GPRS
10. Explain logical channels in GPRS.
11. Explain why PDP context fields stored in MS, HLR, GGSN and SGSN are different and why PDP on text is not stored in VLR.
12. Why does GSM utilize GPRS to carry out location update for circuit switched service?
13. In terms of the number of data links that can be established, what is the difference between GPRS data connection from an MS to external data networks and dial up connection to the data networks?
14. In Alcatel's GPRS solution, every GPRS network is supported by one SGSN and GGSN. In Nortel's solution, several SGSN and GGSN are used to support one GPRS network. Compare these two approaches.
15. How do you implement prepaid service in GPRS?
16. What are different IEEE 802.11 WLAN Standards.
17. Explain primary IEEE 802.11 Specifications and their comparison w.r.t approval date, maximum data rate, modulation, RF band, Number of special streams, channel width.
18. What are the applications of WLAN.
19. Draw and explain IEEE 802.11 WLAN architecture.
20. Compare various IEEE 802.11 standards w.r.t applications, modulation, channel width, typical range, antenna configurations.
21. What is RFID? Discuss some of its applications.
22. Explain RFID components and their characteristics.
23. What are RFID features.
24. What is RFID? Discuss different components of RFID and explain how communication takes place among the components.
25. Explain the risks and benefits of applying RFID in the manufacturing sector. How can it be adopted in tracking parcels for the ecommerce sector.

26. What are advantages and disadvantages of RFID.
27. Define and explain different terms used in Blutooth : Piconet, scatternet, Master unit, slave unit, MAC address, parked unit, sniff and hold mode.
28. Explain the frame format in Bluetooth technology.
29. Explain in detail Bluetooth architecture.
30. Write short note on WiMAX Technology
31. What are salient features supported by Wimax.
32. Explain WiMAX physical layer, WiMAX Medium access control, spectrum allocation for WiMAX, other features of WiMAX.
33. What is the difference between Wi-Fi and WiMAX.
34. What is WiMAX, Explain with its different standards.
35. What are advantages and applications of WiMAX
36. What is Wi-Fi?
37. Explain Wi-Fi working concepts such as radio signals, Wi-Fi cards, Wi-Fi Hotspots.
38. What are various Wi-Fi IEEE Standards.
39. Compare Wi-Fi (802.11b) and Wi-Fi (802.11 a/g)
40. Explain access protocols and control functions in Wi-Fi.
41. Explain Wi-Fi Quality of service
42. Explain Wi-Fi security
43. Explain Wi-Fi network services.
44. What are different Wi-Fi major issues
45. Write short note on mobile IP.
46. How the agent can be discovering using mobile IP? Give the overlay of agent advertisement packet which includes mobility extension
46. What is mobile IP? Explain various components of mobile IP.

✣ ✣ ✣

3... Wireless Application Protocol and 3G Mobile Services

Chapter Outcomes...

- Describe the given specification for compatibility requirements of IMT - 2000 global standards.
- Explain features of the given next generation standard.
- Describe the function of the given section of UMTS network architecture.
- Compare features of the two given next generation mobile communication networks based on given criteria.
- State the procedure of scheduled maintenance of the given system.

Learning Objectives...

- To understand Basic Concepts in WAP
- To learn various 3G Mobile Services
- To understand WML and UMTS Technology
- To study Features of 4G

3.0 INTRODUCTION

- WAP (Wireless Application Protocol) WAP is a universal open standard developed by the WAP forum to provide mobile users of wireless phones and other wireless terminals.
- WAP standard represents the first successful attempt to establish a broadly accepted environment for delivering information, data and services to both enterprise and consumer users over wireless networks.
- WAP is based on existing internet standard such as IP, XML, HTML and HTTP. It also includes security features.
- WAP bridges the gap between mobile world and Internet as well as corporate intranets and offers the ability to deliver an unlimited range of mobile value added services to subscribers-independent of their network, bearer and terminal.
- Mobile subscribers can access the same wealth of information from a pocket-sized device as they can from the desktop.
- WAP is a global standard and is not controlled by any single company. E rricson, Nokia, Motorola and unwired planet founded the WAP forum in the summer of 1997 with the initial purpose of defining an industry-wide specification for developing applications over wireless communications networks.

- The WAP specification define a set of protocols in application, session, transaction security and transport layers, which enable operators, manufacturers and application providers to meet the challenges in advanced wireless service differentiation and fast/flexible service creation.
- WAP also defines an application environment (WAE) aimed at enabling operators, manufacturers and content developers to develop advanced differentiating services and applications including a micro browser, scripting facilities, email, World Wide Web (WWW)-to mobile handset messaging and mobile to telefax access.
- WML stands for Wireless Markup Language. WML is an application of XML, which is defined in a document-type definition. WML is based on HDML and is modified so that it can be compared with HTML. WML takes care of the small screen and the low bandwidth of transmission.
- IMT-2000 Global Standard is emerging Internet environment urgently requires support for asymmetric, interactive, multimedia traffic based on high speed packet data transport.
- Such rapidly growing service requirements given by the global users of requirements, will dramatically change the nature of telecommunication services and the underlying networks in the twenty first century.
- This standard is known as International Mobile Telecommunications-2000 (IMT-2000).where 2000 indicates the target availability data (year 2000) as well as the operational radio frequency band (2000 MHz range) for the standard until 1997,IMT-2000 was known as Future Public Land Mobile Telecommunication Systems (FPLMTS).
- CDMA stands for Code Division Multiple Access. The 3G W-CDMA is based on the network fundamentals of GSM and uses 3G technologies covered in the IMT-2000 global standards.
- UMTS stands for Universe of Mobile Telecommunications System. It is being developed by RACE (Rand in Advanced Communication technologies in Europe) as the Third Generation (3G) wireless system.
- UMTS uses a totally different radio interface based around the use of direct sequence spread spectrum as CDMA (Code division Multiple access).
- In the field of mobile communication services, the 4G mobile services are the advanced version of the 3G mobile communication services.
- Currently in the network technology, one of the most talked terms is Fifth Generation (5G) networks. Although it is well informed that 5G is going to be launched by 2020,but still is a lot of buzz about its upcoming features, additional benefits in comparison to 4G resource requirement to implement the 5G.

3.1 MOBILE INTERNET STANDARD

- WAP utilizes Internet standards such as XML, user datagram protocol (UDP).and IP. Many of the protocols are based on Internet standards such as Hypertext Transfer Protocol (HTTP) and TLS (Transport Layer Security) but have been optimized for the unique constraints of the wireless environment: low bandwidth, high latency and less connection stability.
- Internet standards such as Hypertext Markup Language (HTML), HTTP, TLS and transmission control protocol (TCP)' are inefficient over mobile networks, requiring large amount of mainly text based data to be sent.

- Standard HTML content cannot be effectively displayed on the small size screens of pocket-sized mobile phones and pagers.

3.1.1 WAP Gateway

- The WAP Gateway utilizes Web proxy technology to provide efficient wireless access to the Internet. A proxy plays the roles of both server and client,making requests on behalf of the client.
- Because the WAP handset (a client) can not directly communicate with the origin server(a web server), the WAP Gateway serves as a proxy to handle the requests from the WAP handset,and passes the requests to the origin servers.
- On the Internet side the WAP Gateway translates requests from the WAP protocol stack to the Internet protocol stack (HTTP and TCP/IP).On the wireless network side,the encoder/decoder in the WAP Gateway performs WML text and bytecode conversion to reduce the information transmitted over the wireless networks.
- The WAP Gateway typically supports the DNS service to resolve the domain names used in URLs.It also provides quick response to the WAP handsets by aggregating data from different origin servers,and by caching frequently used information.
- Though the WAP specifications do not specify mechanisms for charging or subscription management, the WAP architecture suggests that appropriate charging information can be collected in the WAP Gateway ,where the WAP security protocol can be used to authenticate the subscriber.
- Although it is not defined in the WAP specifications, WAP Gateway may use the distillation technique to perform on-demand transformation,which effectively reduces the wireless traffic.
- Distillation is highly lossy, real time, data type specific compression that preserves most of the semantic content of a document.It scales down a color image by reducing the number of colors and thus the size of the representation or reduces the frame size,frame rate and resolution of video to create a reduced quality representation.
- The distilled representation allows the user to quickly retrieve a simplified version of an object.If more information of the object is required,refinement is used to fetch extra information to enhance the distilled object.
- Although on-demand transformation increases the latency at the proxy,studies indicate that this technique significantly reduces end to end latency with better output for the clients.
- By installing dynamic adaptation mechanisms in the WAP Gateway,wireless handheld devices can leverage a powerful infrastructure to achieve capabilities they could not achieve on their own.
- The WAP Gateway is a middleware product available on the market.The Motorola WAP Gateway and the Erricson WAP Gateway are based on the windows NT platform.
- APiON and CMG developed their WAP Gateways on the Unix platform.Nokia's WAP Gateways are developed in both Unix and Windows NT.Nokia offers a free download of its WAP Gateway beta product from its Web site,WWW.forum.nokia.com.

3.1.2 WAP Gateway WAP Architecture and Protocols

- The description of WAP Architecture is given below:

WAP Architecture:

- It provides a scalable and extensible environment for application development of mobile. This is achieved using layered design of protocol stack. The layers resemble the layers of OSI model.
- Each layer is accessible by layers above as well as by other services and applications through a set of well defined interface. External applications may access session, transaction, security and transport layers directly.

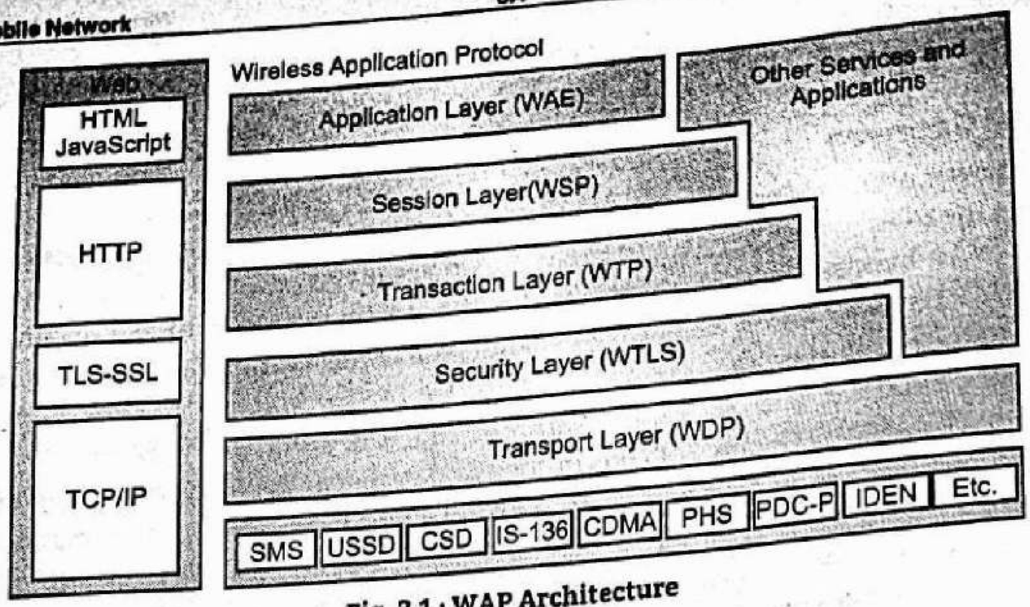


Fig. 3.1 : WAP Architecture

WAP Protocols:

- WAP specifications define a set of lightweight protocols, designed to operate over a variety of wireless bearer services.
- These services can be IP-based (e.g., GPRS and CDPD), or non-IP-based (e.g., SMS and USSD).It is clear that the wireless bearers have very different QOS characteristics.
- The WAP protocols compensate for or tolerate these varying QOS requirements.

1. **Wireless Application Environment (WAE):**

- WAE is the uppermost layer in the WAP stack. It is general purpose environment based on combination of WWW and mobile telephony technologies.
- Its primary objective is to achieve interoperable environment that allows operators and service providers to build applications that can reach wide variety of wireless platforms.
- It uses URL and URI for addressing. Language used is WML and WML script. WML script can be used for validation of user input.

2. **Wireless Telephony Application (WTA):**

- WTA provides a means to create telephony services using WAP. It uses WTA Interface (WTAI) which can be evoked from WML and for WML script.
- The Repository makes it possible to store WTA services in device which can be accessed without accessing the network. The access can be based on any event like call disconnect, call answer etc.
- Sometimes, there can be notification to user based on which WTA services are accessed by users. The notification is called WTA service indication.

3. **Wireless Session Protocol (WSP):**

- WSP provides reliable, organized exchange of content between client and server. The core of WSP design is binary form of HTTP. All methods defined by HTTP 1.1 are supported.
- Capability negotiation is used to agree on common level of protocol functionality as well as to agree on a set of extended request methods so that full compatibility to HTTP applications can be retained.
- An idle session can be suspended to free network resources and can be resumed without overload of full-blown session establishment. WSP also supports asynchronous requests. Hence, multiple requests will improve utilization of air time.

4. **Wireless Transaction Protocol (WTP):**

- WTP is defined as light-weight transaction-oriented protocol suitable for implementation in thin clients.

- Each transaction has unique identifiers, acknowledgements, duplicates removal and retransmission.
- Class 1 and Class 2 enable user to confirm every received message, however, in class 0, there is no acknowledgement.
- WTP has no security mechanisms and no explicit connection set-up or tear-down phases.

5. **Wireless Transport Layer Security (WTLS):**

- WTLS is security protocol based on industry standard transport layer security (TLS). It provides transport layer security between a WAP client and the WAP Gateway/ Proxy.
- The goals of WTLS are data integrity, privacy, authentication, Denial-of-service protection. It has features like datagram support, optimized handshake and dynamic key refreshing.

6. **Wireless Datagram Protocol (WDP):**

- WDP provides application addressing by port numbers, optional segmentation and reassembly, optional error detection.
- It supports simultaneous communication instances from higher layer over a single underlying WDP bearer service. The port number identifies higher level entity above WDP.
- The adaptation layer of WDP maps WDP functions directly on to a bearer based on its specific characteristics. On the GSM SMS, datagram functionality is provided by WDP.

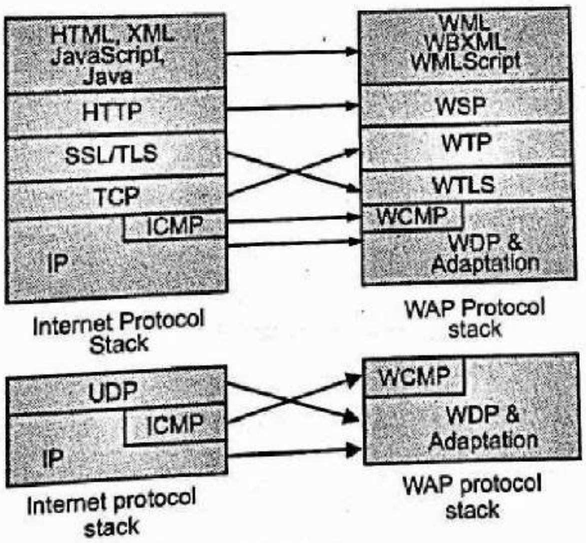
7. **Optimal WAP Bearers:**

- The WAP is designed to operate over a variety of different service like SMS,' Circuit Switched Data (CSD)', GPRS,' Unstructured Supplementary Services Data(USSD)'.

3.1.3 WAP Programming Model

- The similarity with WWW Model, standard components of WAP Programming Model and functionality of WAP Proxy is described in following point.

Similarity with WWW Model:



WML: Wireless Markup Language
WSP: Wireless Session protocol
WTP: Wireless Transport Potocol
WTLS: Wireless Transport Layer Security
WCMP: Wireless Control Management Protocol
WDP: Wireless Datagram Protocol

Fig. 3.2 : WAP Protocol Stack

- WAP is a set of protocols that allow wireless devices like hand-held cell phones to access the internet. But it has programming model similar to that of WWW.
- WAP content and applications are specified in a set of well-known content formats based on WWW content formats

- Transport of content is based on standard communication protocols which are based on that of WWW. The micro browser is analogous to standard web browser.
- Wherever possible, existing standards are adopted, there are also some extensions to match characteristics of wireless environment. This has provided benefits to application developers and ability to use existing tools (e.g., XML tools).

Standard Components of WAP Programming Model:

- **Standard Naming Model:** WWW standard URLs identify WAP content on origin servers and local resources in a device (eg. Call control functions)
- **Content Typing:** All WAP content has a specific type consistent with WWW content types.
- **Standard Content Formats:** WAP content formats are based on WWW technology and include display markup, calendar information, electronic business card objects, images and scripting language.
- **Standard Protocols:** The WAP communication protocols and content types are optimized for mass-market, hand-held wireless devices. The protocols enable the communication of browser requests from mobile terminal to network web server.

Functionality of WAP Proxy:

- WAP utilizes proxy technology to connect between wireless domain and WWW.
  1. **Protocol Gateway:** It translates requests from WAP protocol stack to WWW protocol stack.
  2. **Content Encoders and Decoders:** The encoders translate the content into compact encoded formats to reduce the size of data. Thus, mobile users can browse wide variety of WAP content. Also, application author is able to build applications that run on large number of mobile devices.
  3. **WAP Proxy** allows content and applications to be hosted on WWW servers and to be build using WWW technologies like 'Cell global identity (CGI)' scripting.

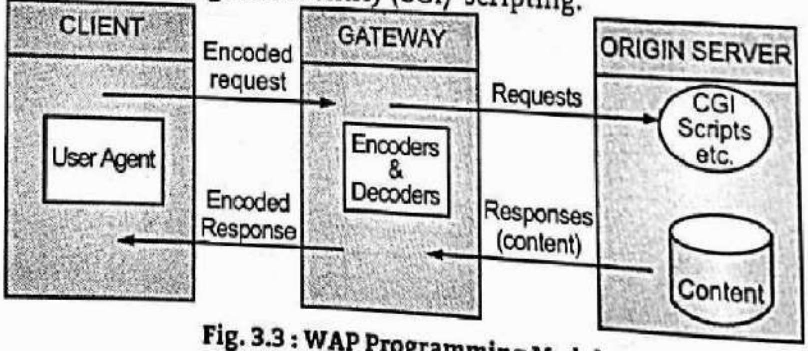


Fig. 3.3 : WAP Programming Model

3.1.4 Advantages, Disadvantages and Applications of WAP

- In this section we will study advantages, disadvantages and applications of WAP.

Advantages of WAP:

1. Implementation near to Internet model.
2. Most modern mobile telephone devices support WAP.
3. Real-Time send/receive data.
4. Multiplatform functionality (little change is needed to run on any website since XMI is used).
5. No hardware obsolescence.

Advantages of WAP 2.0:

1. WAP 2.0 uses 'Cascading Style Sheet (CSS)' plus some WAP specific extensions. CSS is subset of CSS2 which is language of WWW.
2. With WAP 2.0, Web developers can use familiar authoring tools and PC web browsers for building mobile Internet sites.

3. Greater control on appearance of color, background, borders, fonts, etc.
4. If there is only single CSS to whole site, mobile will download it only once when the site is first visited. It is then stored in cache.
5. The layout and formatting information can be moved to separate CSS which makes file size smaller and short download time. Since the content and presentation can be separated:
   - Layout and style of same content can be matched to characteristics of different wireless devices easily and to different user agents easily.
   - The content file need not be modified when new mobile phones come to market. Only layout is modified.
   - A single WAP CSS can be applied to multiple WAP pages.
   - The style code can be used in multiple projects.
   - Work on content and presentation can be divided.

Disadvantages of WAP:

1. Low speeds, security and very small user interface.
2. Not very familiar to users.
3. Business model is expensive.
4. Forms are hard to design.
5. Third party is included.

Disadvantages of WAP 2.0:

1. Different WAP browsers have different levels of support for WAP CSS.
2. An external WAP CSS can increase the time required for a page to be completely loaded the first time WAP Site is Visited because of following Reasons:
3. External WAP CSS style sheet does not exist in cache of mobile at first visit.
4. An XHTML MP document and its external WAP CSS have to be downloaded in separate requests.
5. If a single WAP CSS is used, the file size will be large.
6. The WAP browser needs to parse the CSS in addition to XHTML MP document.

Applications of WAP:

1. The first and foremost application is accessing the Internet from mobile devices.
2. Games can be played from mobile devices over wireless devices.
3. Mobile hand-sets can be used to access time sheets and fill expenses claims.
4. Online banking via mobile phones will be very popular if implemented in secure way.
5. Services like locating WAP customers geographically, providing weather and traffic alerts are possible using WAP.

3.2 WML (WIRELESS MARKUP LANGUAGE)

- WML was designed to describe content and format for presenting data on devices with limited bandwidth, limited screen size, and limited user input capability.
- It is designed to work with telephone keypads, styluses, and other input devises common to mobile, wireless communication.
- WML permits the scaling of displays for use on two line screens found in some small devices, as well as the larger screens found on smart phones.
- For an ordinary PC, a web browser provides contents in the form of web coded with the Hypertext Markup Language (HTML).
- To translate an HTML-coded webpage into WML with content and format suitable for wireless devices, much of the information, especially graphics and animation, must be stripped away.

- . WML presents mainly text based information that attempts to capture the essence of web page and that is organized for easy access for users of mobile devices.

Features of WML:

1. **Text and Image Support:** Formatting and layout commands are provided for text and limited image capability.
2. **Deck/Card Organizational Metaphor:** WML documents are subdivided into small, well-defined units of user interaction called cards. Users navigate by moving back and forth between cards. A card specifies one or more unit of interaction (a menu, a screen of text, or a text entry field). A WML deck is similar to an HTML page in that it is identified by a web address (URL) and is the unit of content transmission.
3. **Support for Navigation Among Cards and Decks:** WML includes provisions for event handling, which is used for navigation or executing scripts. In an HTML-based web browser, a user navigates by clicking on links.

- At a WML capable mobile device, a user interacts with cards, moving forward and back through the deck. WML is tagged language, similar to HTML, in which individual language elements are delineated by lowercase tags enclosed in angle brackets.
- Typically, The WML definition of a card begins with the non visible portion, which contains executable elements, followed the visible content.
- WML Script WML Script is a scripting language with similarities to JavaScript. It is designed for defining script-type programs in a user device with limited processing power and memory.

3.2.1 International Mobile Telecommunications-2000 (IMT 2000)

- IMT-2000 Stands for International Mobile Telecommunications-2000. An initiative of the International Telecommunication Union (ITU) to create a global standard for wireless data networks.
- The goal of International Mobile Telecommunications-2000 (IMT-2000) is to support data transmission rates of up to 2 Mbps for fixed stations and 384 Kbps for mobile stations.
- Note that the "2000" in the term "International Mobile Telecommunications-2000" refers to the transmission speed (approximately 2000 Kbps), not the deployment date (which might be several years beyond the year 2000).
- The European proposal for IMT-2000 prepared by ETSI is called as Universal Mobile Telecommunication System (UMTS).

3.2.2 Features

- The features of IMT-2000 are as follows:
  1. It is used for all radio environments.
  2. It supports both packet switched and circuit switched data transmission.
  3. It offers high spectrum efficiency.
  4. It support wide range of telecommunication services like voice , data, multimedia and internet.

3.2.3 IMT 2000 Architecture

- IMT-2000 is a 3G wireless communications standard defined by the recommendations of the International Telecommunication Vision (ITV).
- Fig. 3.4 shows the IMT 2000 architecture.
- The ITU standardize 5 group of 3G for radio access technology.

1. **IMT-DS:**

- It is used the direct spread technology.
- It is also called Wideband CDMA.
- It is part of Third Generation Partnership Project (3GPP).

2. **IMT-TC:**

- It uses Time Code Technology.
- It further divided into 2 standards TDD and TD-SCDMA.

3. **IMT-MC:**

- It uses Multi Carrier Technology.
- CDMA is multi carrier technology and it is part of 3GPP2.

4. **IMT-SC:**

- It uses Single Carrier Technology.
- It is enhancement of US TDMA System.

5. **IMT-FT:**

- It uses Frequency Time Technology.
- It is enhancement version of the digital cordless telephone standards DECT.

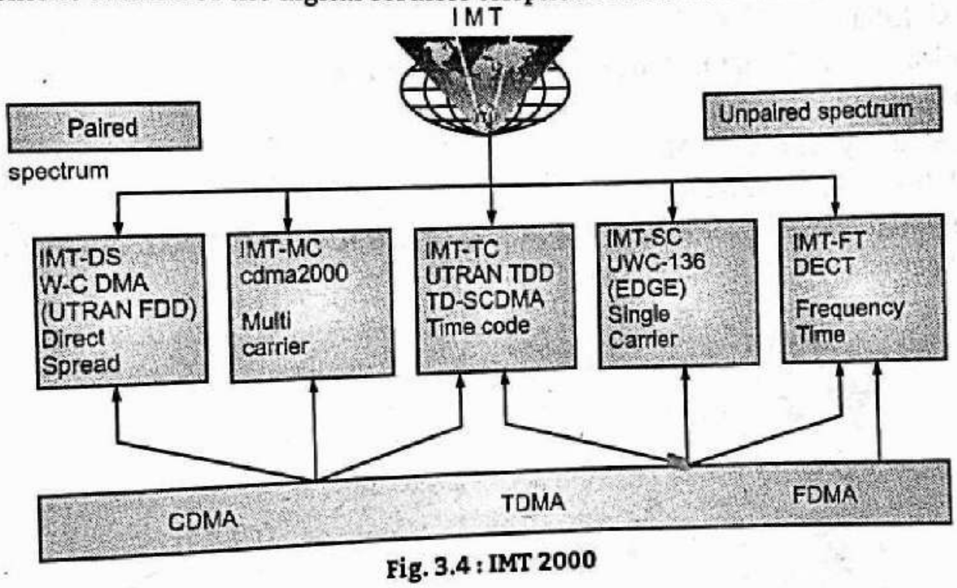


Fig. 3.4 : IMT 2000

3.2.4 IMT 2000 (CDMA 2000) System

- The International Telecommunication Union (ITU), the United National (UN) organization responsible for global telecommunication standards, has been working since 1986 toward developing an international standard for wireless access to worldwide telecommunication infrastructure.
- This standard is known as IMT 2000 or International Mobile Telecommunications 2000 (2000 indicates target availability year 2000 as well as the operational frequency band 2000 MHz range).
- IMT 2000 defines the third generation (3G) mobile telecommunication system which exhibits the following characteristics:
  1. Seamless global mobility and service delivery.
  2. Integration of the wire line and wireless network to provide telecommunication services transparently to the users.
  3. Defining global standards that are flexible enough to meet local needs and to allow current regional/national systems to evolve smoothly towards third generation system.

- The vision for an IMT 2000 system and its Capabilities are:
  1. Common spectrum world-wide (1.8 GHz-2.2 GHz band)
  2. Multiple radio environment (cellular, cordless, satellite, LANs)
  3. Wide range of telecommunication services (voice, data, multimedia and internet)
  4. Flexible radio bearers for increased spectrum efficiency.
  5. Data rates up to 2 Mbps for indoor environments.
  6. Maximum use of IN capabilities.
  7. Global seamless roaming.
  8. Enhanced security and performance.
  9. Integration of satellite and terrestrial systems.
- IMT2000 service environments will address the full range of mobile and personal communication application.
- The scope of IMT2000 services include:
  1. In building (picocell).
  2. Urban (microcell).
  3. Suburban (macrocell).
  4. Global (satellite).
  5. Communication types that include voice, data and images.
- Radio aspects of IMT2000 are:
  1. Uplink frequency: 1885-2025 MHz
  2. Downlink frequency: 2110-2200 MHz
  3. Transmission mode: FDD for mobile and satellite applications and TDD for indoor and pedestrian type applications.

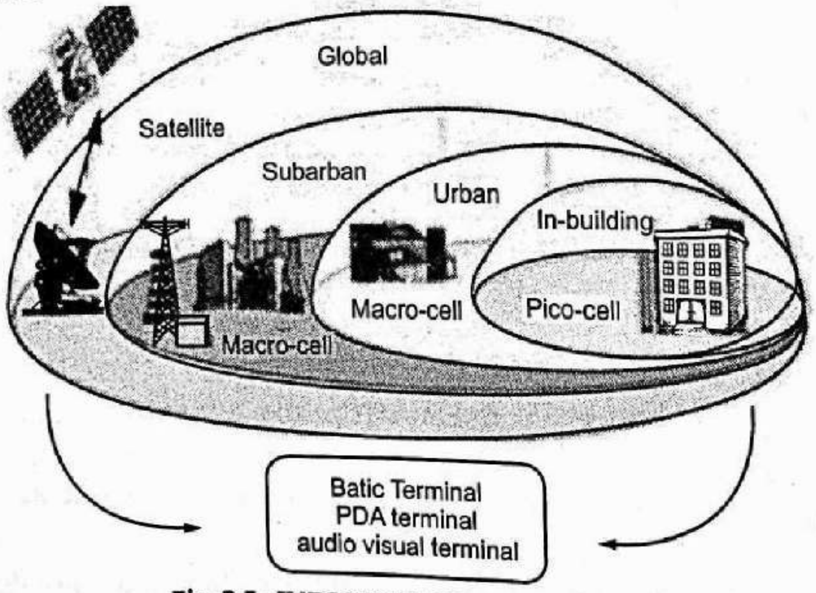


Fig. 3.5 : IMT 2000 (CDMA 2000) System

- A significant element of IMT 2000 is the need to achieve a major improvement in spectrum efficiency compared to the currently available in the 2G mobile communication.
- In context of managing the access the spectrum, sharing a common pool of spectrum between operators and/or between terrestrial and satellite services is used to improve spectrum efficiency.
- Key Features of the Radio Access for IMT 2000 are:
  1. High level of flexibility
  2. Cost effectiveness in all operating environments

3. Commonality of design worldwide
4. Operation within the designated IMT 2000 frequency band

- Global radio channels are scanned by IMT terminal to find the required information on available networks/standards and services.
- These channels carry information like bands used for IMT 2000, frequency rasters, modulation characteristics, guard bands, duplex direction and spacing, list of application services etc.

Network Implementation of IMT 2000:

- As a stand-alone network with gateway and internetworking units towards supporting networks in particular towards PSTN, ISDN, and Packet DATA Networks.
- It may be integrated with the fixed networks. In this functions needed to support specific radio network requirements are integrated to the fixed networks. Base stations are connected directly to a local exchange that can support IMT 2000 traffic by locally integrated functions and by accessing functions in other network elements.
- Requirements for network functions must take into account the support of multimedia services. IMT 2000 system should support global roaming and virtual home environment concept.

IMT 2000 Service and Network Capabilities:

- Circuit and packet bearer capability up to 144 kbps in vehicular radio environment, up to 384 kbps for pedestrian radio environment and up to 2048 kbps for indoor and office radio environment.
- Interoperability and roaming among the IMT 2000 family of systems.
- Service portability and support of virtual home environment.
- Multimedia terminals and services.
- Emergency and priority calls.
- Separation of call and bearer channel/connection control.
- User authentication and ciphering.
- User-network and network-network authentication.
- Geographic position/location service.
- Lawfully authorised electronic surveillance.

IMT 2000 Interfaces for Specifications by the ITU:

- To ensure that systems belonging to different IMT 2000 family members can interoperate to provide seamless global roaming and service delivery.
- MT-RAN interface requires the specifications not only of the physical radio interface but also of layer 2 and layer 3 protocols as well as support some supplication protocol that may be required across this interface.

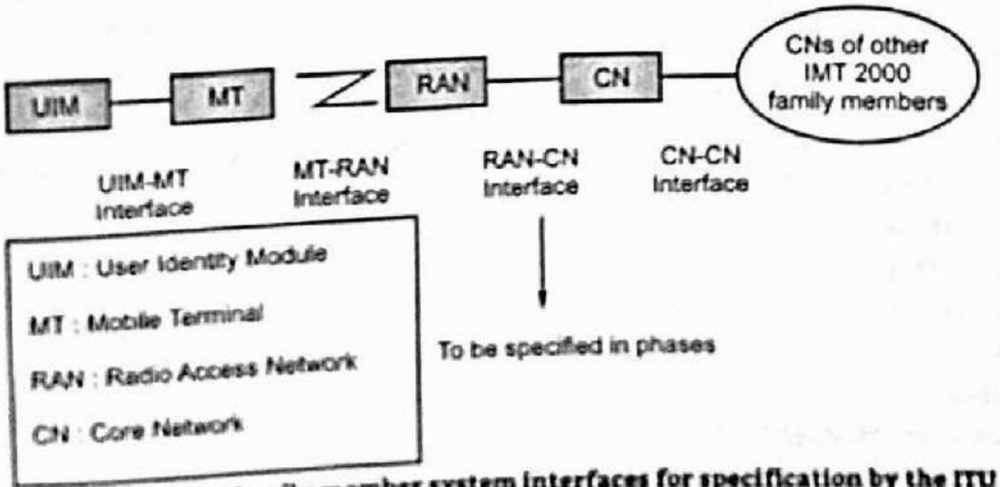

UIM
MT
RAN
CN
CNs of other IMT 2000 family members
UIM-MT Interface
MT-RAN Interface
RAN-CN Interface
CN-CN Interface
UIM : User Identity Module
MT : Mobile Terminal
RAN : Radio Access Network
CN : Core Network
To be specified in phases

Fig. 3.6 : IMT 2000 family member system interfaces for specification by the ITU

- In the initial implementation of IMT 2000 family systems operators may prefer to use RAN-CN interface based on existing wireless PCS systems.

- The UIM-MT interface represents the interface between removable user identity module and the mobile terminal.
- The CN-CN interface is key interface for supporting global roaming across networks belonging to different family members.

3.2.5 IMT 2000 Vision

- IMT-2000 is a global standard to satisfy market demand for mobile service in the twenty-first century.
- The vision for IMT-2000 system services and its capabilities is as under:
  1. Common worldwide spectrum.
  2. Multiple radio environment (LAN, satellite, cordless, cellular).
  3. Worldwide roaming capability.
  4. High quality, enhanced security and performance.
  5. Small terminal for worldwide use.
  6. Integration of satellite and terrestrial system.

3.3 WIDEBAND CODE DIVISION MULTIPLE ACCESS (WCDMA)

- WCDMA stands for Wideband Code Division Multiple Access and is the 3G technology that employs the Direct-Sequence Code Division Multiple Access (DS-WCDMA) channel access method and the Frequency Division Duplexing (FDD) method to provide high-speed and high capacity service
- Third generation (3G) wireless capability has been developed in response to a growing demand in data services.
- There are several different radio access technologies defined within ITU, based on either CDM or TDMA technology. Different regional solutions were proposed as solutions to the requirements of IMT-2000.
- These included Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) utilizing Frequency Division Duplex (FDD) and Time Division Duplex (TDD)
- The fragmentation of the proposals led to the creation of two working groups. One group is known as the Third Generation Partnership Project (3GPP) which is working on the Unified Mobile Telecommunication Standard (UMTS) based on WCDMA.
- The other group is known as 3GPP2 works on CDMA 2000
- Organization 3rd Generation Partnership Project (3GPP) has continued that work by defining a mobile system that fulfils the IMT-2000 standard. This system a called Universal Mobile Telecommunication System (UMTS)
- ITU finally approved a family of five 3G standards which are part of the 3G framework known as IMT-2000. These standards are:
  1. WCDMA (UMTS 99)
  2. WCDMA (HSPA)
  3. CDMA2000
  4. TD-CDMA
  5. TD-SCDMA

WCDMA Features Two Modes:

1. **Frequency Division Duplex (FDD):** Separately users by employing both codes as well as frequencies. One frequency is used for the uplink, while other is used for downlink

2. **Time Division Duplex (TDD): Separates** users by employing codes, frequencies and time wherein the same frequency is used for both uplink and downlink

- WCDMA does no need base station timing synchronization. WCDMA provides significant flexibility to provide support of multiple users at independent data rates. The flexibility necessitates the utilization of multiple complex waveforms for validation and test.

3.3.1 3G CDMA 2000

- Code Division Multiple Access 2000 is the natural evolution of IS-95 (cdma One). It includes additional functionality that increases its spectral efficiency and data rate capability.
- Code Division Multiple Access is a mobile digital radio technology where channels are defined with codes (PN Sequences).
- CDMA permits many simultaneous transmitters on the same frequency channel. Since more phones can be served by fewer cell sites, CDMA –based standards have a significant economic advantage over TDMA or FDMA-based standards.
- This standard is being developed by Telecommunications Industry Association (TIA) of US and is standardized by 3GPP2. The main CDMA 2000 standards are: CDMA 2000 1xRTT,CDMA 2000 1xEV and CDMA 2000 EV-DV.

CDMA 2000 1xRTT:

- RTT stands for Radio Transmission Technology and the designation "1x" meaning "1 times Radio Transmission Technology", indicates the same RF bandwidth as IS-95.The main features of CDMA 2000 1X are as follows:
  1. Supports an instantaneous data rate up to 307 Kbps for a user in packet mode and a typical throughput rates of 144 Kbps per user, depending on the number of user, the velocity of user and the propagating conditions.
  2. Supports up to twice as many voice users a the 2G CDMA Standard.
  3. Provides the subscriber unit with up to two times the standby time for longer lasting battery life.

CDMA 2000 EV:

- This is an evolutionary advancement of CDMA with the following characteristics:
  1. Provides CDMA carriers with the options of installing radio channels with data only (CDMA 2000 EV-DO) and with data and voice (CDMA 2000 EV-DV)
  2. The CDMA 2000 1xEV-DO supports greater than 2.4 Mbps of instantaneous high speed packet throughput per user on a CDMA channel, although the user data rates are much lower and highly dependent on other factors.
  3. CDMA 2000 EV-DV can offer data rates up to 144 Kbps with about twice as many voice channels as IS-95B.

CDMA 2000 3x:

- It is (also known as EV-DO Rev B) is a multi-carrier evolution. It has higher rates per carrier (up to 4.9 Mbps on the downlink per carrier).
- Typical deployments are expected to include 3 Carriers for a peak rate of 14.7 Mbps. Higher rates are possible by bundling multiple channels together. It enhances the user experience and enables new services such as high definition video streaming.
- Uses statistical multiplexing across channels to further reduce latency, enhancing the experience for latency-sensitive services such as gaming, video telephony, remote console sessions and web browsing.

- It provides increased talk-time and standby time. The interference from the adjacent sectors is reduced by hybrid frequency reuse and improves the rates that can be offered, especially to users at the edge of the cell.
- It has efficient support for services that have asymmetric download and upload requirements (i.e different data rates required in each direction) such as file transfers, web browsing, and broadband multimedia content delivery.

3.3.2 CDMA 2000 Evolution Path

- CDMA has single upgrade path for eventual 3G operation. The interim data solution for CDMA is called I-95B. IS-95 channel can support up to 64 user channels. The original IS-95 throughput rate of 9600 bps was improved to current rate 14400 bps.
- The eventual 3G evolution for CDMA system leads to CDMA 2000. Several variants of CDMA 2000 are currently developed but they based on fundamentals of IS-95 and IS-95B technologies.
- The eventual 3G evolution for GSM, IS-136 and PDC system leads to Wideband CDMA (WCDMA), also called Universal Mobile Telecommunication Service (UMTS).
- WCDMA is based on the network fundamentals of GSM as well as the merged versions of GSM and IS-136 through EDGE.
- CDMA2000 standard is based on CDMAone system and allows to access internet by using wireless carrier with high data speed. In the year 2002 the first CDMA 2000 system was offered and standardized by 3GPP2 (3rd Generation Partnership Project 2).
- It is especially used in North America and South America and South Korea. It shares its infrastructure with the IS-95 2G standards. To improve the performance of existing system, the CDMA 2000 does not use any extra equipment. It just only changed the software or hardware of the existing system.
- The CDMA 2000 is more advanced than the CDMAone as it serves the twice number of users than CDMAone and the battery life of mobile station is twice as compared to CDMAone. It also provides high speed data access by using packet data transport.
- CDMA 2000 is seamless and less expensive as compared to W-CDMA. CDMA 2000 also known as IMT-CDMA. Multi-carrier is a CDMA version of the IMT-2000 standard developed by the International Telecommunication Union (ITU).
- CDMA 2000 is a set of standards that define the new air interface and changed in radio access that will enhance the network capacity, improve data speed and bandwidth of mobile terminals and also allow end-to-end IP services.
- In early 1990s the application of CDMA technology was introduced in cellular system with development and characterization of IS-95 standard. The CDMA 2000 technology is developed from IS-95 with significant enhancement in voice capacity, data speed rate and network features.
- The 3G system implement soft handoff when MS moves from one location to another to overcome the problem of near far terminal.
- CDMA 2000 is backward compatible with IS-95 that include enhancement in access and traffic state handoff. The CDMA 2000 family reuses the existing IS-95 service standards such as those that define speech services, Short Message Services.
- Data rates of up to 150 kbps or 300 kbps is provided that depend on the configuration of traffic channel radio, enhanced channel coding with turbo encoders at higher data rates are used. It has increased mobile terminal battery life with the introduction of new quick paging channel.
- All above features are used in CDMA 2000 to provide a voice capacity that is twice that of the CDMAone systems and data rate of 153.6 kbps or 307.2 kbps depending on the radio configuration used.

3.3.3 Services Provided by CDMA 2000 Cellular Technology

- The services provided by CDMA 2000 Cellular Technology are as follows:
  1. Code Division Multiple access 2000 is the neutral evolution of IS-95. (CDMAOne). It includes additional functionality that increase its spectral efficiency and data rate capability.
  2. CDMA is a method in which multiple users occupy the same time and frequency allocations and are channelized by unique assigned codes. The signals are separated at the receiver by using a correlator that accepts only signal energy from the assigned Code Channel. The channels are defined with codes (PN sequences). All other signals in that frequency band contribute only to the noise.
- Three main CDMA 2000 standards are:
  1. CDMA 2000 1Xrtt
  2. CDMA 2000 1Xev
  3. CDMA 2000 EV-DC
- CDMA 2000 1Xrtt support both voice and data services over the standard 1.25MHz CDMA channel. The 1x in the name signifies that it uses one 1.25MHz channel. Due to improved modulation, power control, and overall design, it can achieve theoretical data transfer rates of 144Kbps
- There are two members of CDMA 2000 1Xev Family:
  1. CDMA2000 1x Evolution Data Optimized
  2. CDMA2000 1x Evolution Data and Voice
- The CDMA2000 1x EVDO supports greater than 2 Mbps of instantaneous high speed packet throughput per user on a CDMA channel, although the data rates are much lower and highly dependent on other factors.
- The CDMA2000 1x EVDV can offer data rates up to 144 kbps with about twice as many voice channels as IS-95B.
- Base station timing synchronization in CDMA 2000 can provide decreased latency and a reduced chance of dropping calls during soft handoff.
- Since both WCDMA and CDMA 2000 have been simultaneously adapted for the 3G standard, harmonization of these two systems becomes necessary to make IMT-2000 deployment successful.
- To create a single integrated 3G CDMA specification and process the separate W-CDMA and CDMA proposals being developed by 3GPP and 3GPP2.

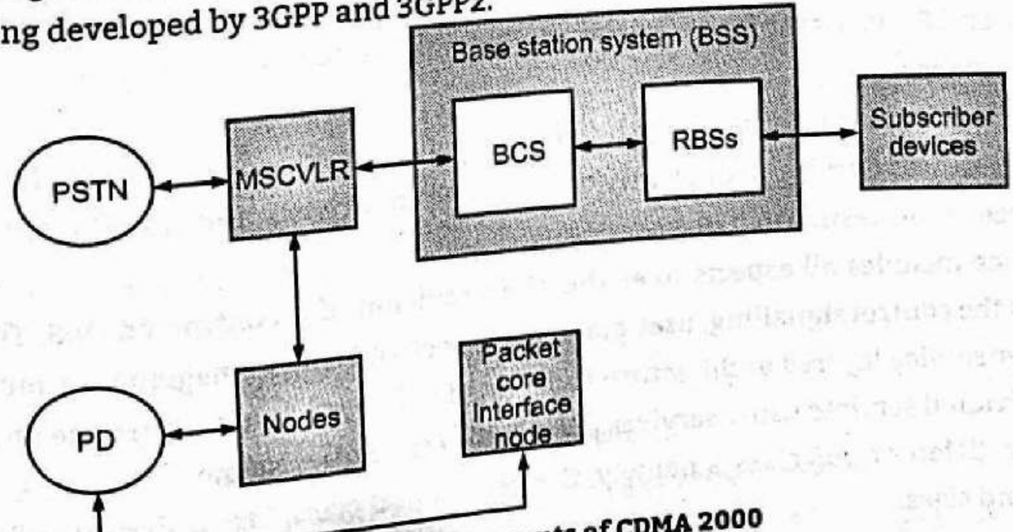


Fig. 3.7: Components of CDMA 2000

3.3.4 Comparison of CDMA 2000 and WCDMA

- CDMA 2000 is a 3G technology evolved from IS-95 CDMA technique. WCDMA is a 3G technology evolved from GSM technology.

Table 3.1

Terms	CDMA 2000	WCDMA
Core network	ANSI-41 MAP	GSM MAP
Channel bandwidth	1.25 MHz (1X), 3.75 MHz (3X)	5.0 MHz
Channelization codes	4-128 (1X), 4-256 (3X)	4-256
Chip rate	1.2288 Mcps (1X), 3.6864 Mcps (3X)	4.096 Mcps (DOCOMO), 3.84 Mcps (UMTS)
Synchronized base station	Yes	No; but synchronized BS is Optional
Frame length	5 ms (signaling), 20, 40, 80 ms physical layer frames	10 ms for physical layer, 10,20, 40, and 80 ms for transport Layer
Multi-carrier spreading option	Yes, but in cdma2000 1X (direct spread)	No (direct spread)
Modulation	QPSK (forward link), BPSK (reverse link)	QPSK (both links)
Modes of operation	FDD	FDD and TDD
Source identification code for Sector	One PN code (32,768 chips),512 unique offsets are generated, using PN offsets	512 unique scrambling codes, each identifying a sector,(38,400 chips)
Source identification code for Mobile	One long PN code (242242) chips, unique offsets are generated, based on ESN, not assigned, by sector	Unique scrambling codes assigned by sector

3.3.5 Quality of Services in Third Generation (QoS in 3G)

- Network Services are considered end-to-end, this means from a Terminal Equipment (TE) to another TE. An End-to-End Service may have a certain Quality of Service (QoS) which is provided for the user of a network service.
- It is the user that decides whether he is satisfied with the provided QoS or not. To realise a certain network QoS a Bearer Service with clearly defined characteristics and functionality is to be set up from the source to the destination of a service.
- A bearer service includes all aspects to enable the provision of a contracted QoS. These aspects are among others the control signalling, user plane transport and QoS management functionality.
- A UMTS bearer service layered architecture is depicted below, each bearer service on a specific layer offers it's individual services using services provided by the layers below.
- There are four different QoS classes namely, Conversational class, Streaming class, Interactive class and Background class.

Table 3.2

Traffic Class	Conversational class	Streaming class	Interactive class	Background class
	Real Time	Real Time	Best Effort	Best Effort
Fundamental characteristics	Preserve time relation (variation) between information entities of the stream	Preserve time relation (variation) between information entities of the stream	Request response pattern	Destination is not expecting the data within a certain time
	Conversational pattern (stringent and for delay)		Preserve payload content	Preserve payload content
Example of the application	Voice	Streaming video	Web browsing	Telemetry, emails

3.4 UMTS TECHNOLOGY

- UMTS stands for Universe of Mobile Telecommunications System. To handle a mixed range of traffic, a mixed cell layout that would consist of microcells overlaid on microcells and picocells is one of the architecture plans being considered.
- This type of network distributes the traffic with the local traffic operating on the microcells and picocells, while the high mobile traffic is operated on the microcells. Thus, reducing the number of hand-offs required for the fast moving traffic.

3.4.1 UMTS Features

- The features of UMTS are as follows:
  1. Bandwidth : 5 MHz or 1.25 MHz.
  2. Chip rate : 3.84 Mcps.
  3. Frame duration : 10 to 20 ms (frame length).
  4. Data rate : 2.048 Mbps.
  5. Frame structure : 16 slots per frame.
  6. Backward compatibility : GSM.
  7. Power control frequency : 1.5 MHz.
  8. Base station synchronization: Asynchronous.
  9. Data rate: up to 144 Kbps.
  10. Antenna used: Simple Antenna.
  11. Frequency spectrum: Uplink 1920 to 1980 MHz.
  12. Downlink 2110 to 2170 MHz.
  13. Duplexing Technique : FDD and TDD modes.
  14. Modulation scheme : Direct sequence CDMA with QPSK.
  15. Coding Technique : Orthogonal Variable Spreading Factor (OVSF).
  16. Service type : Multirate and multiservice.

3.4.2 UMTS Network Architecture

- With the changes from 2G to 3G,the emphasis for the systems changed from focus on mobile voice communications to mobile data and general connectivity.
- The foundation for the UMTS network had been set in place when GSM was launched. This provided the basic access elements as well as circuit switched voice.
- The additional network entities to be added it was the combination of these two network elements that provided the basis for 3G UMTS network architecture.
- A UMTS system can be divided into a set of domains and the reference points that interconnect them.
- The UMTS network architecture is partly based on existing 2G network components and some new 3G network components. It inherits the basic functional elements from the GSM architecture on the Core Network (CN) side.
- The MS of GSM is referred as User Equipment (UE) in UMTS. The MSC has quite similar functions both in GSM and UMTS. Instead of circuit-switched services for packet data, a new packet node SGSN is introduced. This SGSN is capable of supporting data rates of up to 2 Mbps.
- The core-network elements are connected to the radio network via the Iu interface, which is very similar to the A-interface used in GSM.
- The major changes in the UMTS architecture are in the Radio Access Network (RAN), which is also called UMTS Terrestrial RAN (UTRAN). There is a totally new interface called Iur, which connects two neighbouring Radio Network Controllers (RNCs). BSs are connected to the RNC via the Iub interface.

UMTS Terrestrial RAN (UTRAN)

- UTRAN consist of Radio Network Subsystems (RNSs). The RNS has two main elements:
  1. Radio Network Controllers (RNC)
  2. Node B

1. **Radio Network Controller (RNC):**

- The RNC is responsible for control of the radio resources in its area. One RNC controls multiple nodes B.
- The RNC in UMTS provides functions equivalent to the Base Station Controller (BSC) functions in GSM/GPRS networks.
- The major difference is that RNCs have more intelligence built-in than their GSM/GPRS counterparts. For example, RNCs can autonomously manage handovers without involving MSCs and SGSNs.

2. **Node B:**

- The Node B is responsible for air-interface processing and some radio-resource management functions.
- The Node B in UMTS networks provides functions equivalent to the base transceiver station (BTS) in GSM/GPRS networks. UMTS operates at higher frequencies than GSM/GPRS and therefore the signal coverage range is less.

Features of UMTS Interfaces:

- The UMTS interfaces can be categorized as follows:

1. **Uu** is the interface between the user equipment and the network. That is, it is the UMTS air interface. The equivalent interface in GSM/GPRS networks is the um interface.
2. **The Iuis** split functionally into two logical interfaces, Iups connecting the packet switched domain to the access network and the Iucs connecting the circuit switched domain to the access network. The standards do not dictate that these are physically separate, but the user plane for each is different and the control plane may be different.

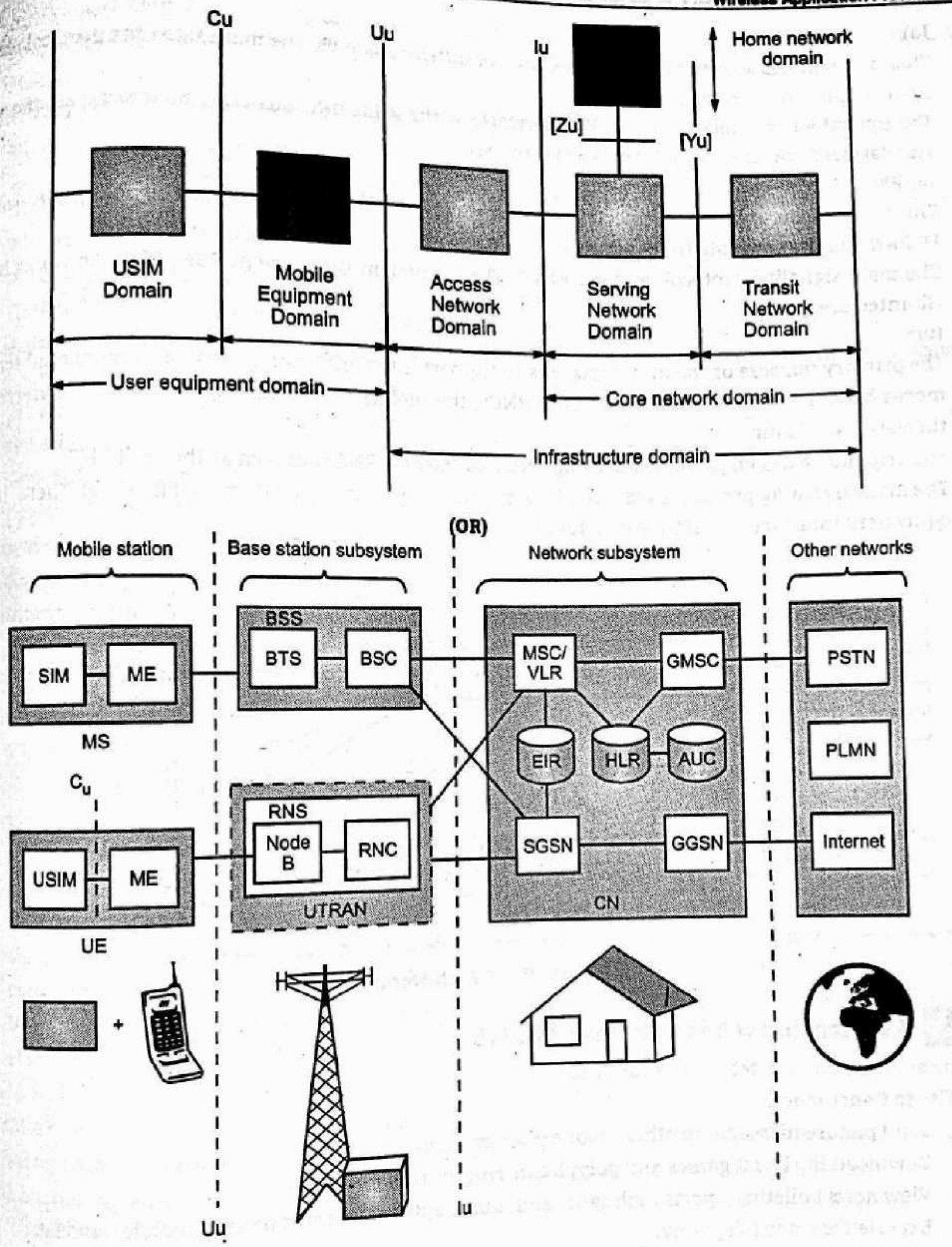


Fig. 3.8 : UMTS Architecture

3. **Iu -CS:**

- This is the circuit-switched connection for carrying (typically) voice traffic and signaling between the UTRAN and the core voice network.
- The main signaling protocol used is Radio Access Network Application Part (RANAP). The equivalent interface in GSM/GPRS networks is the A-interface.

4. **Iub:**

- This is the interface used by an RNC to control multiple Node Bs. The main signaling protocol used is Node B Application Part (NBAP).
- The equivalent interface in GSM/GPRS networks is the A-bis interface. The Iub interface is the main standardized and open, unlike the A-bis interface.

5. **Iu -PS:**

- This is the packet-switched connection for carrying (typically) data traffic and signaling between the UTRAN and the core data GPRS network.
- The main signaling protocol used is RANAP. The equivalent interface in GSM/GPRS networks is the Gb-interface.

6. **Iur:**

- The primary purpose of the Iur interface is to support inter-MSC mobility. When a mobile subscriber moves between areas served by different RNCs, the mobile subscriber's data is now transferred to the new RNC via Iur.
- The original RNC is known as the serving RNC and the new RNC is known as the drift RNC.
- The main signaling protocol used is Radio Network Subsystem Application Part (RNSAP). There is no equivalent interface in GSM/GPRS networks.

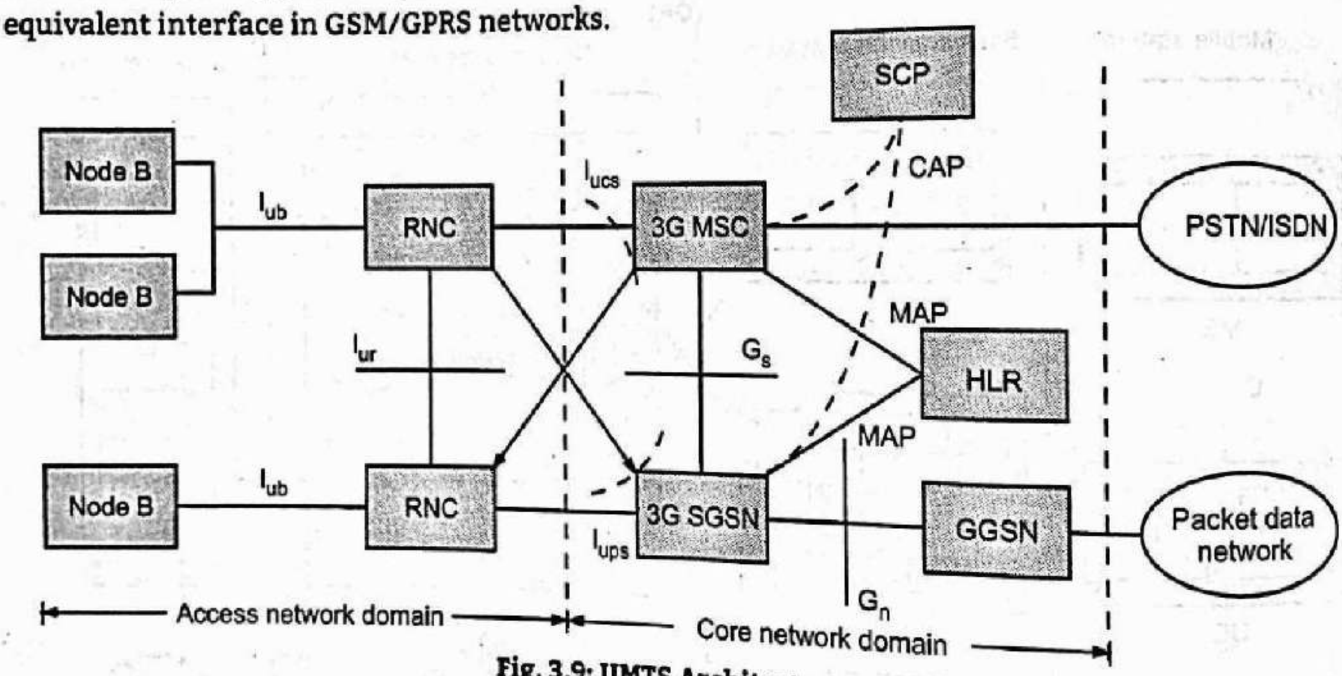


Fig. 3.9: UMTS Architecture

3.4.3 Applications/Advantages of UMTS

- The applications of UMTS are as follows:-

Benefits to Consumers:

1. Send picture messages to other mobile phones.
2. Download the latest games and polyphonic ringtones.
3. View news bulletins, sports highlights and music videos streamed to their mobile handset.
4. Experience video telephony.

- List of Possible Type of Services that will be Available in 3G Networks:
  1. **Fun:** WWW, video, post card, snapshots, text, picture and multimedia messaging, datacast, personalisation applications (ring tone, screen saver, desk top),juke box, virtual companion/pet.
  2. **2Work:** Rich call with image and data stream, IP telephony,B2B ordering and logistics, information exchange, personal information manager, dairy, scheduler, note pad,2-way video

conferencing, directory services, travel assistance, work group, telepresence, FTP, instant voicemail, colour fax.

3. **Media:** Push newspaper and magazines, advertising, classified
4. **Shopping:** E-commerce, e-cash, e-wallet, credit card, tele-banking, automatic transaction, auction, microbilling shopping.
5. **Entertainment:** News, stock market, sports games, lottery, gambling, music, video, concerts, adult content.
6. **Education:** Online libraries, search engines, remote attendance, field research.
7. **Peace of Mind:** Remote surveillance, location tracking, emergency use.
8. **Health:** Telemedicine, remote diagnose and health monitoring.
9. **Automation:** Home automation, traffic telematics, machine-machine communication (telemetry).
10. **Travel:** location sensitive information and guidance, e-tour, location awareness, time tables, e-ticketing.
11. **Add-on:** TV, radio, PC, access to remote computer,MP3 player, camera, video camera, watch, pager, GPS, remote control unit.

Benefits to Operators:

1. Automatic international roaming.
2. Integral security and billing functions.
3. Retaining many of the existing back-office systems.
4. Flexibility to introduce new multimedia services to business users and consumers while providing an enhanced user experience.
5. Higher demand for value added services and a corresponding increase in revenues.
6. Support more subscribers-especially in urban areas where existing 2G networks are facing limitations.
7. Offer data speed up to 10 times higher than GPRS in order to enable new multimedia services such as video telephony.
8. Building on current investments in GSM/GPRS,3G/UMTS offers mobile service operators significant capacity and broadband capabilities to support greater number of voice and data customers-especially in urban areas-plus higher data rate at lower incremental cost than 2G.
9. Various research and development work is going on to achieve throughput speed beyond 3G standard like RAN,HSDPA,HSUPA.

- These technologies will play an instrumental role in positioning 3G/UMTS as a key enabler for true 'mobile broadband'.
- Offering data transmission speed of same order of magnitude as today's Ethernet based networks that are mostly used by the fixed line operators to provide broadband services.
- 3G/UMTS will offer enterprise customers and consumers all the benefits of broadband connectivity whilst on the move.

3.5 FOURTH GENERATION (4G)

- 4G (2013) is a high speed data rate plus voice system. The 4G mobile communications will have transmission rates up to 20Mbps higher than that of 3G.

- 4G technology is expected to provide very smooth global roaming universally with lower cost. Theoretically 4G is set to deliver 100 Mbps to a roaming mobile device globally and up to 1Gpbs to a stationary device.
- 4G will bring almost perfect real world wireless internetworking called WWWW (Worldwide Wireless Web).
- With the expected features in mind 4G allows for video conferencing, streaming picture perfect video (eg. tele-medicine and tele-geo processing application) and much more.
- 4G uses variable spreading factor-orthogonal frequency and code Division Multiplexing (VSF-OFCDM) and Variable Spreading Factor Code-Division Multiple Access (VSF-CDMA).

4G Features:

- 4G technology is basically the extension in the 3G technology with more bandwidth and services offered in the 3G features of 4G are:
  1. 4G support for interactive multimedia, voice, streaming video, internet and other broadband services.
  2. 4G is IP based mobile system.
  3. 4G has high speed, high capacity and low cost per bit.
  4. 4G has global access, service portability and scalable mobile services.
  5. 4G has seamless switching and a variety of Quality of service driven services.
  6. 4G has better scheduling and call admission control techniques.
- A short history of cellular evolution from 1G to 4G cellular systems is shown in table.

Table 3.3

Technology	Various Generations				
	1G	2G	2.5G	3G	4G
Design began	1970	1980	1985	1990	2000
Implementation	1984	1991	1999	2002	2012-2015
Service	Analogue voice	Digital voice	High-capacity packets, MMS	High-capacity broadband data	Higher capacity, completely IP, Multimedia
Multiple Access	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	OFDMA
Standards	AMPS, TACS, NMT	CDMA, GSM, PDC	GPRS, EDGE	WCDMA, CDMA 2000	Single standard
Bandwidth	1.9 Kbps	14.4 Kbps	384 Kbps	2Mbps	200 Mbps
Core Network	PSTN	PSTN	PSTN, Packet network	Packet network	Internet

3.5.1 VoLTE and its Features

- It is a standard for high speed wireless communication for mobile phones and data terminals including IOT devices and wearables.
- It is based on the IP Multimedia Subsystem network, with specific profiles for control and media planes of voice service on LTE defined by GSM in PRD IR.gz.
- Voice over Long Term Evolution (VoLTE) is a standard for high speed wireless communication for mobile phones and data terminals-including IoT (Internet of Things) devices and wearables.

- It is based on the IP Multimedia subsystem network with specific profiles for control and media planes of voice service on LTE (Long Term Evolution) is a standard for high-speed wireless communication for mobile devices and data terminals defined by GSMA (Global System for Mobile Association).
- Fig. 3.10 shows architecture of VoLTE system.

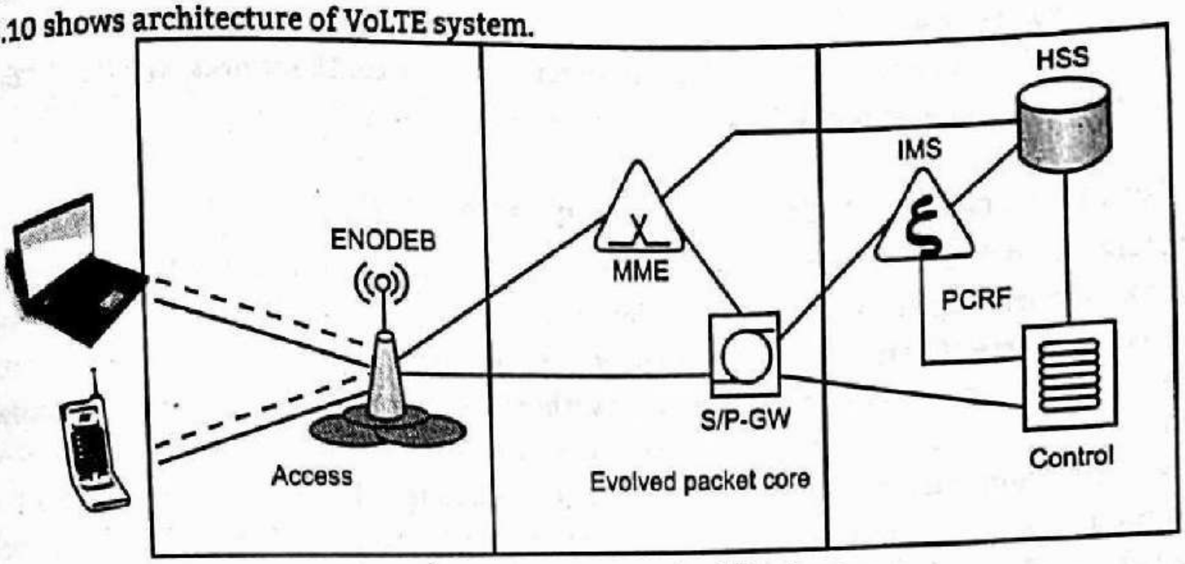


Fig. 3.10 : VoLTE System Architecture

ENODEB : Evolved Node B.

MME : Mobility Management Entity.

S/P-GW : Serving/PDN(Packet Data Network) Gateway.

HSS : Home Subscriber Server.

IMS : IP Multimedia Subsystem.

PCRF : Policy and Charging Rules Functions.

- Voice over LTE(VoLTE) aims to provide the ability to handle cellular voice calls over LTE. Most major network providers have announced their intensions to at least begin to deploy VoLTE within the next couple years.

VoLTE Features:

1. Set up of the transmission path between the terminal and IMS.
2. Security features for user authentication providing.
3. Providing the core functionality for the establishment and termination of the call(via SIP).
4. Support to call forwarding ,caller ID presentation and restriction, call waiting and multiparty conference.
5. Designed for both voice and data traffic.

3.5.2 Advantages and Disadvantages of VoLTE

- The advantages and disadvantages of VoLTE are as follows:-

Advantages of VoLTE:

1. It delivers all voice and data services over same network. Hence it does not require to maintain legacy infrastructure.
2. VoLTE make calls much faster compare to 2G/3G voice calls.
3. It offers better security and QoS (Quality of Service) compare to legacy 2G/3G networks.
4. Delivers an unusually clear calling experience.
5. Provides rapid call establishment time.

Disadvantages of VoLTE:

1. It requires investment in network wide IMS. Hence this will not be available everywhere and hence roaming could be challenge for sometime.
2. If there is no data connection or 4G signaling in the area, user will neither be able to call nor able to use internet using handset.
3. VoLTE should be supported by handsets in order to obtain VoLTE services. The VoLTE feature is not available in all mobile handsets.

3.5.3 Next Generation of Mobile Communication (5G)

- The rapidly increasing number of mobile devices, voluminous data and higher data rate are pushing to rethink the current generation of the cellular mobile communication. The next or fifth generation 5G cellular networks are expected to meet high end requirements.
- The 5G networks are broadly characterized by three unique features: ubiquitous connectivity. Extremely low latency and very high speed data transfer.
- 5G is a generation currently under development. It denotes the next major phase of mobile telecommunications standards beyond the current 4G/IMT Advanced standards.5G networks will also need to meet the needs of new use-cases such as Internet of Things (IoT) as well as broadcast like services and lifeline communications in times of disaster.
- 5G (2021) mobile technology has changed the means to use cellphones within very high bandwidth.
- Now days mobile users have much awareness of the cellphone (mobile) technology. The 5G technologies include all types of advanced features which make 5G mobile technology most powerful and in huge demand in near future.

Features of 5G:

1. The 5G technology is providing up to 25Mbps connectivity speed.
2. 5G technology offer high resolution for crazy cell phone user and bi-directional large bandwidth shaping.
3. 5G technology also providing subscriber supervision tools for fast action.
4. The advanced billing interfaces of 5G technology makes it more attractive and effective.
5. The high quality services of 5G technology based on policy to avoid error.
6. The traffic statistics by 5G technology makes it more accurate.
7. 5G technology is providing large broadcasting of data in Gigabit which supporting almost 65,000 connections.
8. The remote diagnostics also a great feature of 5G technology.
9. 5G technology offer transporter class gateway with unparalleled consistency.
10. Through remote management offered by 5G technology a user can get better and fast solution.
11. The 5G technology network offering enhanced and available connectivity just about the world.

3.5.4 4G Architecture

- 4G stands for fourth generation cellular system. 4G is evaluation of 3G to meet the forecasted rising demand.
- It is an integration of various technologies including GSM,CDMA,GPRS,IMT-2000 ,Wireless LAN. Data rate in 4G system will range from 20 to 100 Mbps.

Features:

1. Fully IP based Mobile System.
2. It supports interactive multimedia, voice, streaming video, internet and other broadband service.

3. It has better spectrum efficiency.
4. It supports Ad-hoc and multi hop network.

4G Architecture:

- Fig. 3.11 shows Generic Mobile Communication architecture.4 G network is an integration of all heterogeneous wireless access networks such as Ad-hoc, cellular, hotspot and satellite radio component.
- Technologies used in 4G are smart antennas for multiple input and multiple output (MIMO), IPv6, VoIP, OFDM and Software Defined Radio (SDR) System.

Smart Antennas:

- Smart Antennas are Transmitting and receiving antennas.
- It does not require increase power and additional frequency.

IPV6 Technology:

- 4G uses IPV6 Technology in order to support a large number of wireless enable devices.
- It enables a number of application with better multicast, security and route optimization capabilities.

VoIP:

- It stands for Voice over IP.
- It allows only packet to be transferred eliminating complexity of 2 protocols over the same circuit.

OFDM:

- OFDM stands for Orthogonal Frequency Division Multiplexing.
- It is currently used as WiMax and WiFi.

SDR:

- SDR stands for Software Defined Radio.
- It is the form of open wireless architecture.

Advantages:

- It provides better spectral efficiency.
- It has high speed, high capacity and low cost per bit.

Disadvantage:

- Battery usage is more.
- Hard to implement.

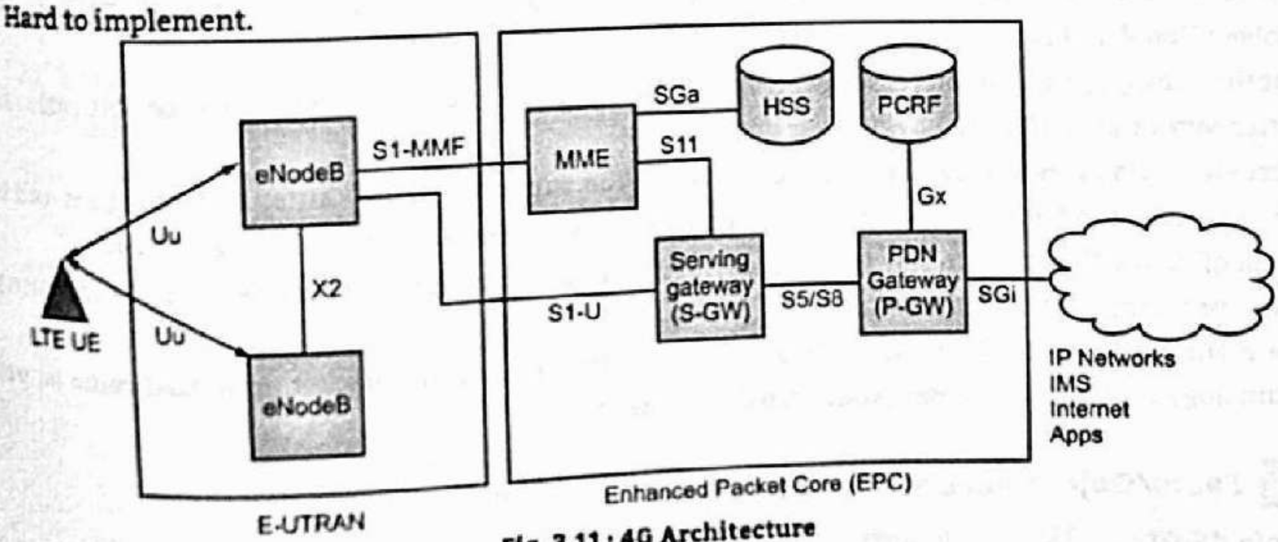


Fig. 3.11 : 4G Architecture

MME- Mobility Management Entity:

It is used for Paging , Authentication, Handover and Selection of Serving Gateway

SGW- Serving Gateway:

It is used to Routing and Forwarding user data packet.

PDN-GW Packet Data Network Gateway:

It is used for User Equipment (UE) IP allocation.

HSS -Home Subscriber Server:

It is a user Database used for service subscriber, user identification and addressing

PCRF -Policy and Charging Rule Function:

It provide quality of service and charging

eNode B-evolved Node B:

It is used as radio resources management and radio bearer control.

3.5.5 LTE

- LTE stands for Long Term Evolution and it was started as a project in 2004 by telecommunication body known as the Third Generation Partnership Project (3GPP).
- SAE (System Architecture Evolution) is the corresponding evolution of the GPRS/3G packet core network evolution. The term LTE is typically used to represent both LTE and SAE.
- Long Term Evolution is the next step forward in cellular 3G services. LTE enhanced the Universal Mobile Telecommunication Services (UMTS) in asset of points on account of the future generation cellular technology needs and growing mobile communication services requirements.
- LTE evolved from an earlier 3GPP system known as the Universal Mobile Telecommunication System (UMTS) which is turn evolved from the Global System of Mobile Communication.
- Even related specifications were formerly known as the evolved UMTS Terrestrial Radio Access (E-UTRA) and evolved UMTAS terrestrial radio access network (E-UTRAN). First version of LTE was documented in Release 8 of the 3GPP specifications.
- A rapid increase of mobile data usage and emergence of new applications such as MMOG (Multimedia Online Gaming), mobile TV, Web 2.0, streaming contents have motivated the 3rd Generation Partnership Project (3GPP) to work on LTE on the way towards 4th Generation mobile.
- LTE offers a reduced latency delay, which is achieved with a simplified flat radio infrastructure in which some of the functions have been moved from the Radio Network Controller (RNC) to the evolved NodeB (eNB)
- Another design goal is to increase spectrum efficiency and as such as a better cost per bit ratio and better service provisioning.
- Increased data rates will be realized the including the support of multi antenna techniques and in combination with techniques such as Orthogonal Frequency Division Multiplexing (OFDM).
- It will offer the flexibility in spectrum deployment and provide higher robustness against frequency selective fading for the system.
- The main goal of LTE is to provide a high data rate, low latency and packet optimized radio access technology supporting flexible bandwidth deployments.

3.5.6 Facts/Objective/Details of LTE

- The objectives of LTE are as follows:
  1. LTE is the successor technology not only of UMTS but also of CDMA 2000.
  2. LTE is important because it will bring up to 50 times performance improvement and much better

3. LTE introduced to get higher data rates, 300Mbps, peak downlink and 75Mbps peak uplink. In a 20Mhz carrier data rates beyond 300Mbps can be achieved under very good signal conditions.
4. LTE is an ideal technology to support high data rates for the services such as VoIP. Streaming multimedia, video conferencing or even high speed cellular modem.
5. LTE uses both Time Division Duplex (TDD) and Frequency Division Duplex (TDD) mode. In FDD uplink and downlink transmission used different frequency, while in TDD both uplink and downlink use the same carrier and same separated in time.
6. LTE supports flexible carrier bandwidths, from 1.4Mhz up to 20Mhz as well as both FDD and TDD. LTE designed with a scalable carrier bandwidth from 1.4Mhz up to 20Mhz which bandwidth is used depends on the frequency band and the amount of spectrum available with a network operator.
7. All LTE devices have to support (MIMO) Multiple Input and Multiple Output transmissions, which allow the base station to transmit several data streams over the same carrier simultaneously.
8. All interfaces between network nodes in LTE are now IP based, including the backhaul connection to the radio base stations. This is great simplification compared to earlier technologies that were initially based on E1/T1, ATM and frame relays links, with most of them being narrowed and expensive.
9. Quality of Service(QoS) mechanism have been standardized on all interfaces to ensure that the requirement of voice calls for a constant delay and bandwidth can still met when capacity limits are reached.
10. Works with GSM/EDGE/UMTS systems existing 2G and 3G spectrum and new spectrum. Supports hand-over and roaming to existing mobile networks.

3.5.7 4G-LTE Architecture

- The high-level network architecture of LTE is comprised of following three main components:
  1. The User Equipment (UE).
  2. The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
  3. The Evolved Packet Core (EPC).
- The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:

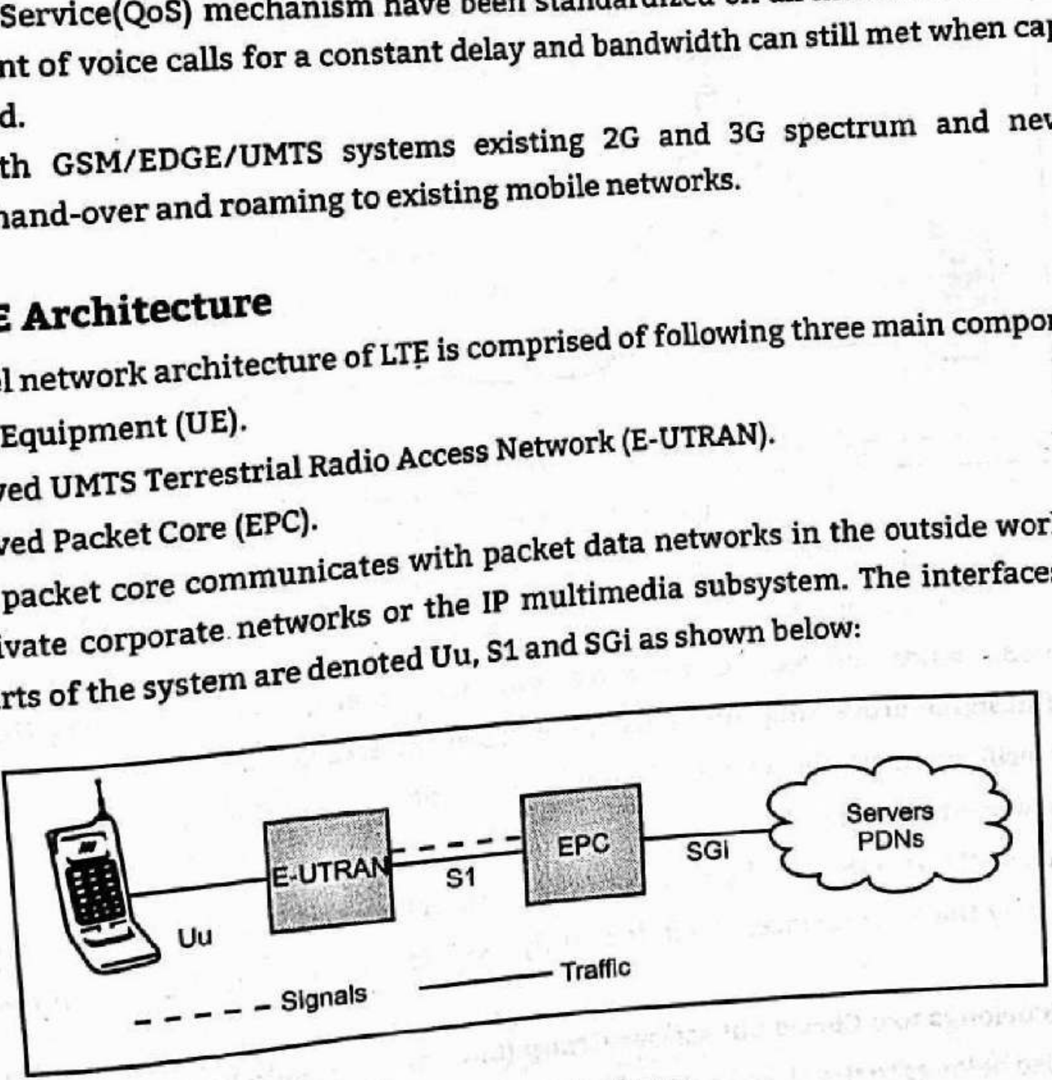


Fig. 3.12 : Interfaces

User Equipment (UE):

- The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME).
- The mobile equipment comprised of the following important modules:
  1. **Mobile Termination (MT) :** This handles all the communication functions.
  2. **Terminal Equipment (TE) :** This terminates the data streams.
  3. **Universal Integrated Circuit Card (UICC) :** This is also known as the SIM card for LTE equipment's. It runs an application known as the Universal Subscriber Identity Module (USIM).

E-UTRAN (The Access Network):

- The architecture of evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated below:
  - o The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called eNodeB or eNB. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

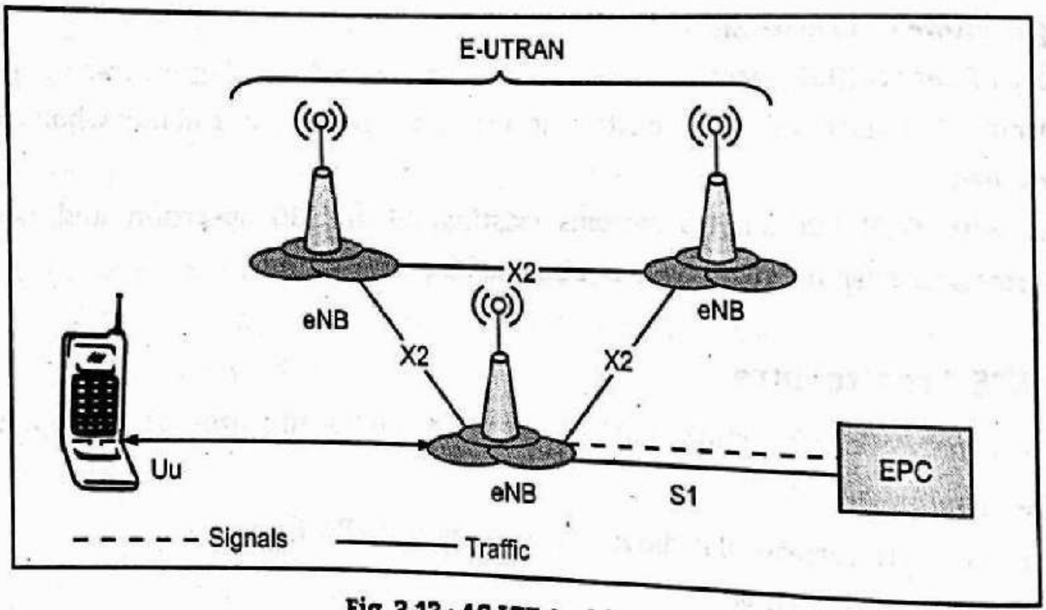


Fig. 3.13 : 4G LTE Architecture

  - o LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:
    1. The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
    2. The eNB controls the low-level operation of all its mobiles, by sending them signaling messages such as handover commands.
- Each eBN connects with the EPC by means of the S1 interface and it can also be connected to nearby base stations by the X2 interface, which is mainly used for signaling and packet forwarding during handover.
- A home eNB belongs to a Closed Subscriber Group (CSG) and can only be accessed by mobiles with a USIM that also belongs to the closed subscriber group.

Evolved Packet Core (EPC)/Core Network:

- The architecture of Evolved Packet Core (EPC) has been illustrated below:

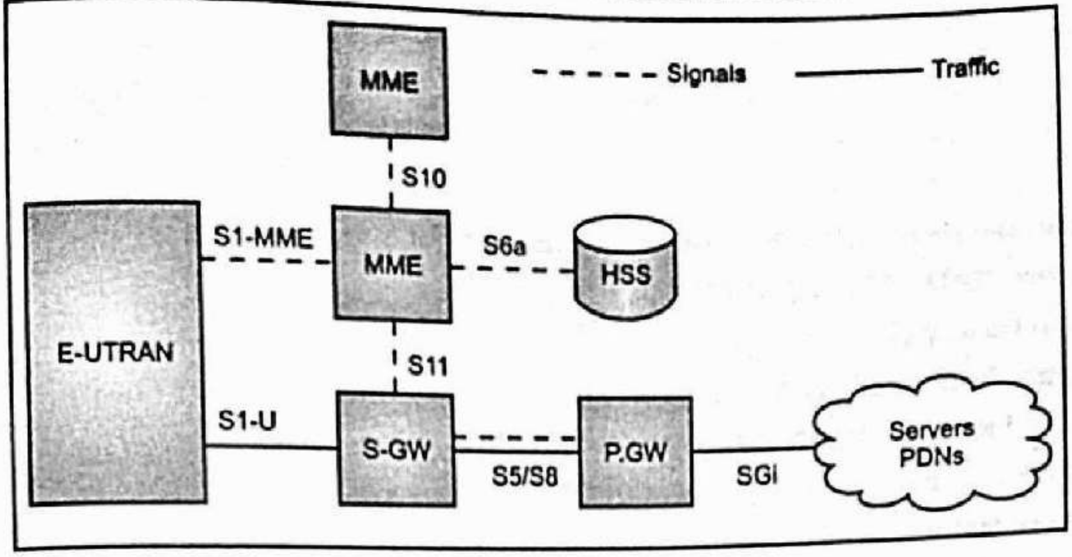


Fig. 3.14 : EPC Architecture

- A brief description of each of the components shown in the above architecture:
  - The Home Subscriber Server (HSS) component has been carried forward from UMTS and GSM and is a central database that contains information about all the network operator's subscribers.
  - The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world that is packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN). The PDN gateway has the same role as the GPRS support node (GGSN) and the serving GPRS support node (SGSN) with UMTS and GSM.
  - The serving gateway (S-GW) acts as a router, and forwards data between the base station and the PDN gateway.
  - • The Mobility Management Entity (MME) controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS). The interface between the serving and PDN gateways is known as S5/S8. This has two slightly Different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.
  - LTE thus aims to provide a peak data rate of 100 Mbps in downlink and 50 Mbps in Uplink respectively.

Practice Questions

1. What are the design guidelines for WAP? What are the disadvantages of implementing TCP/IP directly over the mobile network?
2. Describe the WAP protocol stack. In which situation is WTP not used?
3. Describe distillation. Which layer of WAP implements this mechanism?
4. What is a user agent profile? What happens if a user agent profile is not used in WAP? How can distillation and a user agent profile be used together?
5. What are different mobile Internet standard in WAP?
6. Explain WAP Gateway?
7. Describe WAP architecture with diagram and its associated protocols.
8. Explain WAP programming model in detail.

4...

WLL, Signal Encoding Techniques and Spread Spectrum Modulation

Chapter Outcomes...

- Describe the given application of wireless local loop.
- Explain features of the given signal encoding technique for wireless network.
- Compare PCM, DPCM, DM modulation techniques on the given criteria.
- Describe characteristics of the given spread spectrum modulation technique.
- State the procedure of scheduled maintenance of the given system.

Learning Objectives...

- To understand Basic Concepts WLL with its Architecture
- To learn Signal Encoding Techniques
- To study signal Spread Spectrum Modulation
- To learn LEC Networks

4.0 INTRODUCTION

- Wireless Local Loop (WLL) is a generic term for an access system that uses wireless link rather than conventional copper wire to connect subscribers to the local telephone company's switch.
- WLL is also known as Fixed Wireless Access (FWA) or simply fixed radio. This type of system uses analog or digital radio technology to provide telephone, facsimile, and data services to business and residential subscribers.
- WLL systems provide rapid deployment of basic phone service in areas, where the terrain or telecommunications development makes installation of traditional wirelines service too expensive.
- WLL systems can be easily integrated in to a wireline Public Switched Telephone Network (PSTN) for more quickly than the traditional wireline installations.
- Electrical representation of binary codes is called "line code". A line code is a chosen for use within a communications system for transmitting a digital signal down a transmission line.
- Line coded signal is used to create an "RF signal" that can be sent through free space. The line-coded signal can be converted to bits on an optical disc.

4.1 WLL ARCHITECTURE

- WLL stands for Wireless Local Loop. Microwave wireless links can be used to create a wireless local loop as shown in Fig. 4.1.

Operation:

- Wireless Local Loop (WLL) is a new communications access method that uses radio waves for transmission of information between customers and service provider sites, rather than traditional fixed methods such as copper or fiber optic.
- The architecture consists of three major components namely, Wireless Access Network Unit (WANU), Wireless Access Subscriber Unit (WASU) and Switching Function (SF).

1. **Wireless Access Network Unit (WANU):**

- It is an interface between underlying telephone network and wireless link that consists of Base Station Transceivers (BTS) or Radio Ports (RP), Radio Port Controller Unit (RPCU) or BSC Access Manager (AM), Home Location Register (HLR).

BS:

- It is a base station of WLL system.

RPCU:

- Radio Port Control Unit that connects a number of cell site based station transceivers and associated antennas. The RPCU provides the interface between the base stations and a telephone switch.
- It provides control and signaling functions for implementing the air interface to wireless handsets through the base stations.

Access Manager (AM)

- The Access Manager/Home Location Register (AM/HLR) handles authentication and privacy

2. **Wireless Access Subscriber Unit (WASU)**

- It is located at the subscriber. It translates wireless link into a traditional telephone connection.
- It provides an air interface toward the network and another interface to the subscriber. This interface includes protocol conversion and transcoding, authentication functions.

3. **Switching Function (SF)**

- It can be a digital switch. All the SF includes ISDN algorithms. It is the transmission link between WANU and SF can be microwave or cable.

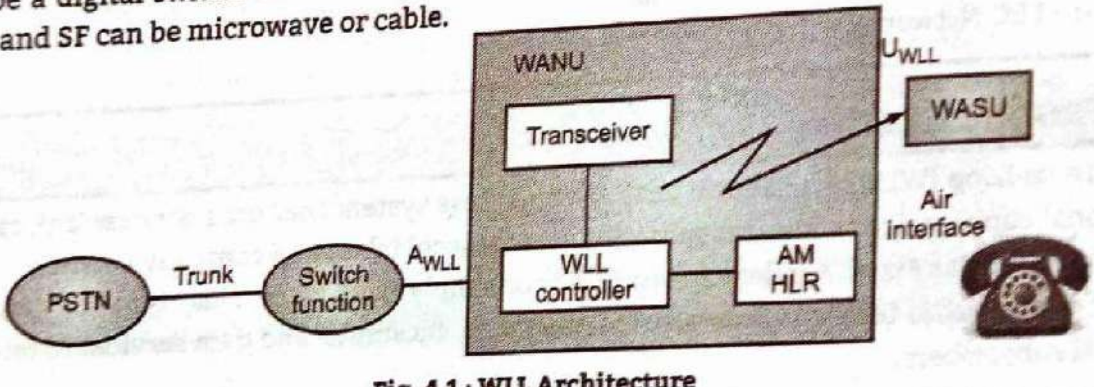


Fig. 4.1 : WLL Architecture

4.1.1 WLL MAJOR TECHNOLOGIES

- The WLL system can be based on 4 major technologies. They are:

1. **Satellite-Based Systems:**

- These systems provide telephony services for rural communities and isolated areas such as islands. Satellite systems are designed for a Gaussian or Rician channel with K factor greater than 7 dB.
- These systems can be of two types **Technology designed specifically for WLL applications** and **Technology piggy backed onto mobile satellite systems as an adjunct service** of these.
- The former offers quality and grade of service comparable to wireline access, but it may be expensive.
- The latter promises to be less costly but, due to bandwidth restrictions, may not offer the quality and grade of service comparable to plain old telephone service (POTS).

- An example of a satellite based technology specifically designed for WLL is the HNS Telephony Earth Station (TES) technology.

Advantages:

1. Low bit rate for voice and data.
2. Low cost mobile terminals.
3. It provides quality and grade of service for WLL applications.

Disadvantages:

1. The number of satellites and propagation delay put restrictions on the system design.
2. Handover capability is needed e.g. LEO, MEO satellites are in motion relative to the earth's surface, so they need handover capability for all fixed and cellular applications

2. Cellular-Based Systems:

- These systems provide large power, large range, median subscriber density, and median circuit quality WLL services. Cellular WLL technologies are primarily used to expand the basic telephony services.
- This approach offers both mobility and fixed wireless access from the same cellular platform.For relatively sparsely populated rural and even urban settings, WLL technologies based on existing cellular systems can be economical and rapidly deployable.
- They include much sophisticated technology and therefore overhead band width not necessarily required for the WLL application. The resultant limited user bandwidth represents a fundamental limitation of such systems for WLL.

Advantages:

1. They provide fixed wireless access and mobility.
2. They can be rapidly deployed in rural and urban areas.
3. They provide large power and operating range.
4. They provide medium circuit and medium subscriber density.

Disadvantages:

1. They are not recommended for deployment of indoors and in picocells.
2. Air interface is complex.
3. The user bandwidth is limited.

3. Fixed Wireless Access Systems

- These systems are proprietary radio systems designed specifically for fixed wireless applications, which may or may not be extensible to PCS or cordless.
- The primary disadvantage of the cellular approach is its limitation on toll quality voice (new toll-quality vocoders designed for cellular technologies may eliminate this problem), and signaling transparency.
- The primary disadvantage of low-tier PCS and microcellular approaches is their range. FWA systems for zonal areas are designed to cover the local telephone area directly from the PSTN switches.
- The systems for rural areas provide connection at the remote ends of rural links to the end users.

Advantages:

1. Less expensive
2. It can be easily installed
3. The installation time need is less.

Disadvantages:

1. Limitation on toll-quality and signaling transparency.

4. Low-Tier PCS or Microcellular-Based Systems:

- These systems provide low power, small range, high subscriber density, and high circuit quality WLL services. These technologies are considered to facilitate rapid market entry and to expand the capacity of the existing infrastructure.
- They are typically operated at 800 MHz, 1.5 GHz, 1.8 GHz, and 1.9 GHz frequency bands. Compared with the cellular-based WLL, more base stations are required to cover the same service area.
- Operators may consider low-tier WLL technologies when an existing infrastructure is in place to support backhaul.
- For densely populated urban environments, WLL technologies based on existing low-tier PCS radio technologies.

Advantages:

1. High Subscriber density.
2. Low power.
3. High circuit quality.

Disadvantages:

1. Transmission cost is more.

4.1.2 WLL Types (FWT and WT with Mobility)

- There are two types of WLL:FWT (Fixed Wireless Telephone) and WT with Mobility as described in this section.

FWT (Fixed Wireless Telephone):

- WLL systems re simpler form of cellular mobile systems. They utilize the frequency re-use concept but without handing over concept. They are used to provide large number of subscribers with a fixed telephone service within a short period of time. Omni directional or sectorial antennae, typically 60 degrees are installed at the central stations whereas the subscribers stations can use simple directional antennae.
- FWT systems are short distance systems connecting subscribers by radio with a nearby exchange (up to 15Km away) or outside line plant access cable termination point (typically 300m to 3Km away). FWT systems are basically part of access network from exchange to subscriber.

WT with Mobility:

- These systems still provide a local terminal mobility since communication is possible within the confines of the cell in which the subscriber is located. The major cordless systems are given below.
  1. British cordless Telephone System(CT-2)
  2. Digital European Cordless Telecom System(DECT)
  3. Japanese Personal Handy Phone System(PHS)
  4. North American Personal Access Communication System.
- Without going in to the details of the above systems, it may be noted that Indian Institute of Technology, Chennai has developed an indigenous system in 1800 MHz band known as CORDECT.
- It has a range of about 3Km and has bright prospects for usage as replacement to local loop between telephone exchange and subscriber. This system has already been successfully introduced in the local network.

4.1.3 WLL Application

- WLL applications includes:
  1. Local phone service via wireless connection
  2. Cheaper to install than wired lines.
  3. Very prominent in non-industrialized nations.

Table 4.1 : Radio Parameters of CT-2,DECT and PHS

Parameter	CT-2	DECT	PHS
Standard	ETSI	ETSI	Lapanese
Frequency MHz	864-868	1880-1900	1895-1918
Access Method	FDMA	MC TDMA	MC TDMA
Voice Chls per car	1	12	4
RF chl spacing	100 KHz	1.728MHz	300 KHz
Voice coding Algorithm	ADPCM	ADPCM	ADPCM
Voice coding rate	32 Kbps	32 Kbps	32 Kbps
Channel bit rate	72 Kbps	1152 Kbps	384 Kbps
Modulation	2 level FSK	GFSK	Pi/4 QPSK

4.2 CONCEPT OF LEC NETWORKS

- LEC (Local Exchange carrier) is the term for a public telephone company in the U.S that provides local service.
- Some of the largest LECs and the Bell operating companies which were grouped in to holding companies known collectively as the Regional Bell Operating Companies (RBOCs) when the Bell system was broken up by a 1983 consent decree. In addition to the Bell companies, there are a number of independent LECs, such as GTE.
- LEC Companies are also sometimes referred to as "telcos" A "local exchange" is the local "central office" of an LEC. Lines from homes and businesses terminate at a local exchange.
- Local exchanges connect to other local exchanges within a Local Access and Transport Area (LATA) or to Inter Exchange Carriers (IXCs) such as long distance carriers. AT&T, MCI and Sprint.

4.3 LINE CODING TECHNIQUES

- Line coding is a process of converting binary data (a sequence of bits) to a suitable format for transmission through the channel with minimum probability of errors.
- Fig. 4.2 shows classification of line coding.

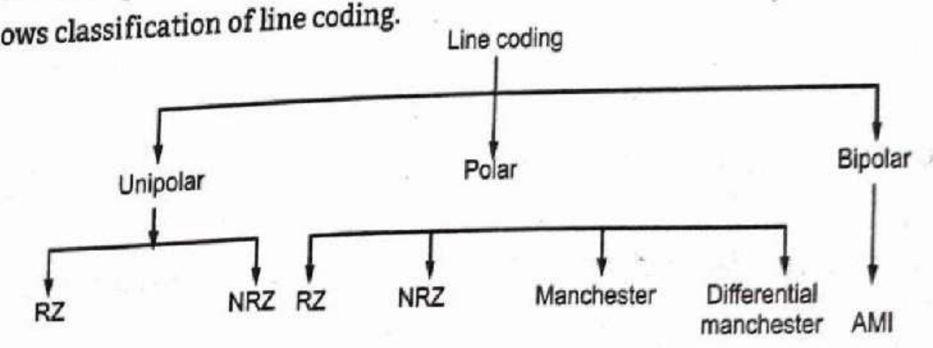


Fig. 4.2 : Classification of Line coding

Unipolar Non-Return to Zero (NRZ): In this type of unipolar signaling, a High in data is represented by a positive pulse called as Mark, which has a duration T_0 equal to the symbol bit duration. A Low in data input has no pulse.

Unipolar Return to Zero (RZ): In this type of unipolar signaling, a High in data, though represented by a Mark pulse, its duration T_0 is less than the symbol bit duration. Half of the bit duration remains high but it immediately returns to zero and shows the absence of pulse during the remaining half of the bit duration.

Bipolar Signaling: This is an encoding technique which has three voltage levels namely +, - and 0. Such a signal is called as duo-binary signal. An example of this type is Alternate Mark Inversion (AMI). For a 1, the voltage level gets a transition from + to – or from – to +, having alternate 1s to be of equal polarity. A 0 will have a zero voltage level. Even in this method, we have two types namely Bipolar NRZ and Bipolar RZ. From the models so far discussed, we have learnt the difference between NRZ and RZ. It just goes in the same way here too.

4.3.1 Advantages and Disadvantages of Encoding Techniques

Advantages of Unipolar:

1. Simple mechanism to generate signal

Disadvantages of Unipolar:

1. **DC component:**The average amplitude of unipolar encoded signal is not zero. It has a DC component associated with it. This component affects the between of the processing circuit and also the power required to transmit the signal through the media.
2. **Synchronization:**A series of same kind of bits can cause a problem while decoding. When signal is not varying, the receiver cannot determine the beginning and ending of each bit. Whenever there is no signal change to indicate the start of next bit, the receiver has to depend on time. The lack of synchronization between the transmitter and receiver clock distorts the signal. This disadvantage is overcome by using parallel lines which carry clock pulse and allows receiver to synchronize with transmitter. This increases the cost and hence not used.

Advantages of NR-I:

1. DC component is reduced because two voltage levels are present. Since 1's are represented. As a transition, synchronization is achieved for consecutive 1's.

Disadvantages of NR-I:

1. Synchronization for consecutive 0's is not achieved.

Advantages of Biphase:

1. At least 1 transition in 2 bit period which can be used for synchronization.
2. The waveform doesn't have DC component because every bit is encoded as +ve polarity for half bit period and –ve polarity for half bit period.
3. Error detection is easier because there is at least 1 transition for each bit.

Disadvantages of Biphase:

1. The frequency at which transitions are taking place is high, and hence higher bandwidth requirement.

4.3.2 Properties of Line Codes or State Factors Deciding Selection of Line Codes

- Properties of line codes or factors deciding selection of line codes are explained in this section.

1. **D.C Component:**

- All communication channels do not allow transmission of dc signal. Line code signal must have zero average value i.e. zero dc component.

- If the channel has poor low frequency response the signal should not have dc or low frequency content. NRZ group signals are having more dc component whereas phase encoded signal will have low dc contents.

2. **Self Clocking Capability:**
- Irrespective of information bit sequence line code used should take at least one transition during each bit interval.
- These transitions are used by receivers for synchronizations with transmitter.

3. **Error Detection:**
- This feature of line code helps to identify the errors in the received signal .
- Multilevel binary group codes provides self error detection capability.

4. **Bandwidth Compression:**
- Line code used should take the minimum necessary bandwidth for transmission.
- The multilevel codes requires less bandwidth as compared to other codes.

5. **Differential Encoding:**
- Line code generated using differential encoding is useful for those communication system where transmitted waveform sometimes experiences an inversion.
- For example, differential machester.

6. **Transperancy:**
- It should be possible to correctly tetrive data regardless of the pattern of one's and zero's.
- Phase encoded having good transparency.

7. **Noise Immunity:**
- Ability to reject noise called noise immunity. Line codes used should have very high noise immunity.
- The NRZ format have better noise immunity than that of other codes because they will have high average power.

8. **Minimum Crosstalk:**
- Line codes should be such that at low frequencies it should have low average power to minimize crosstalk between adjacent channels.
- RZ group signal provides minimum crosstalk.

Comparison of Unipolar RZ and Unipolar NRZ Encoding Scheme

Table 4.2

Unipolar RZ	Unipolar NRZ
In this format each "0" is represented by an off pulse(0)and each "1" by an on pulse With amplitude A and duration $T_b/2$.	In this format each "0" is represented by an off pulse(0)and each "1" by an on pulse With amplitude A and duration T_b.
During the on time, the pulse return to zero after half bit period.	During the on time, the pulse does not return to zero after half bit period.
Unipolar RZ pulses carry less energy.	Unipolar NRZ pulses carry more energy.
Clock recovery is Poor.	Clock recovery is Good.
Synchronization is not essential.	Synchronization is not essential.

4.3.3 Guidelines to Draw Line Codes

- Guidelines to draw line codes waveforms are as follows:-
  1. **NRZ-L:** One is represented by one level, zero is represented by other level

2. **NRZ-M:** One is represented by change in polarity and zero is represented by no change in polarity.
3. **NRZ-S:** One is represented by no change in polarity and zero is represented by change in polarity.
4. **Unipolar NRZ:** One is represented by high level and zero is represented by zero level.
5. **Unipolar RZ:**One is represented by half bit width pulse and zero is represented by no pulse condition.
6. **Polar RZ (Bipolar RZ):** One and zero are represented by opposite level polar pulses that are one half bit in width.
7. **RZ AMI:** One is represented by show half wave ,for alternate one change polarity and zero is represented by zero level.
8. **Bi-ϕ-L (Biphase Level or Split Phase Manchester):** One is represented by 10 and zero is represented by 01.
9. **Bi-ϕ-M (Biphase Mark):**
    - A transitions occurs at beginning of every bit period.
    - One is represented by second transition one half bit period later.
    - Zero is represented by No second transition.
10. **Bi-ϕ-S (Biphase Space):**
    - A transition occurs at the beginning of every bit period.
    - One is represented by no second transition.
    - Zero is represented by second transition one half bit period later.
11. **Dicode NRZ:**
    - A One to zero or zero to one change polarity. Otherwise zero is sent.
12. **Dicode RZ:**
    - A One to zero or zero to one transition produces a half duration polarity change.
    - Otherwise zero is sent.
13. **Delay Mode:**
    - One is represented by transition at the midpoint of the bit interval.
    - Zero is represented by no transition unless it is followed by another zero.
    - In this case a transition is placed at the end of bit period of the first zero.
14. **Polar Quaternary:**
    - Two bits are grouped together.

	Level
00	-3A/2
01	-A/2
10	A/2
11	3A/2

15. **Gray coded:** Two bits are grouped together.

	Level
00	−3A/2
01	−A/2
11	A/2
10	3A/2

16. **Differential Manchester:**

- Transition at middle of every bit interval
- Zero is represented using transition at beginning.

Draw RZ, NRZ Manchester and Differential Manchester line code waveform for data stream 10100110.

Note: RZ and NRZ both Unipolar or Polar or Bipolar waveform should be considered

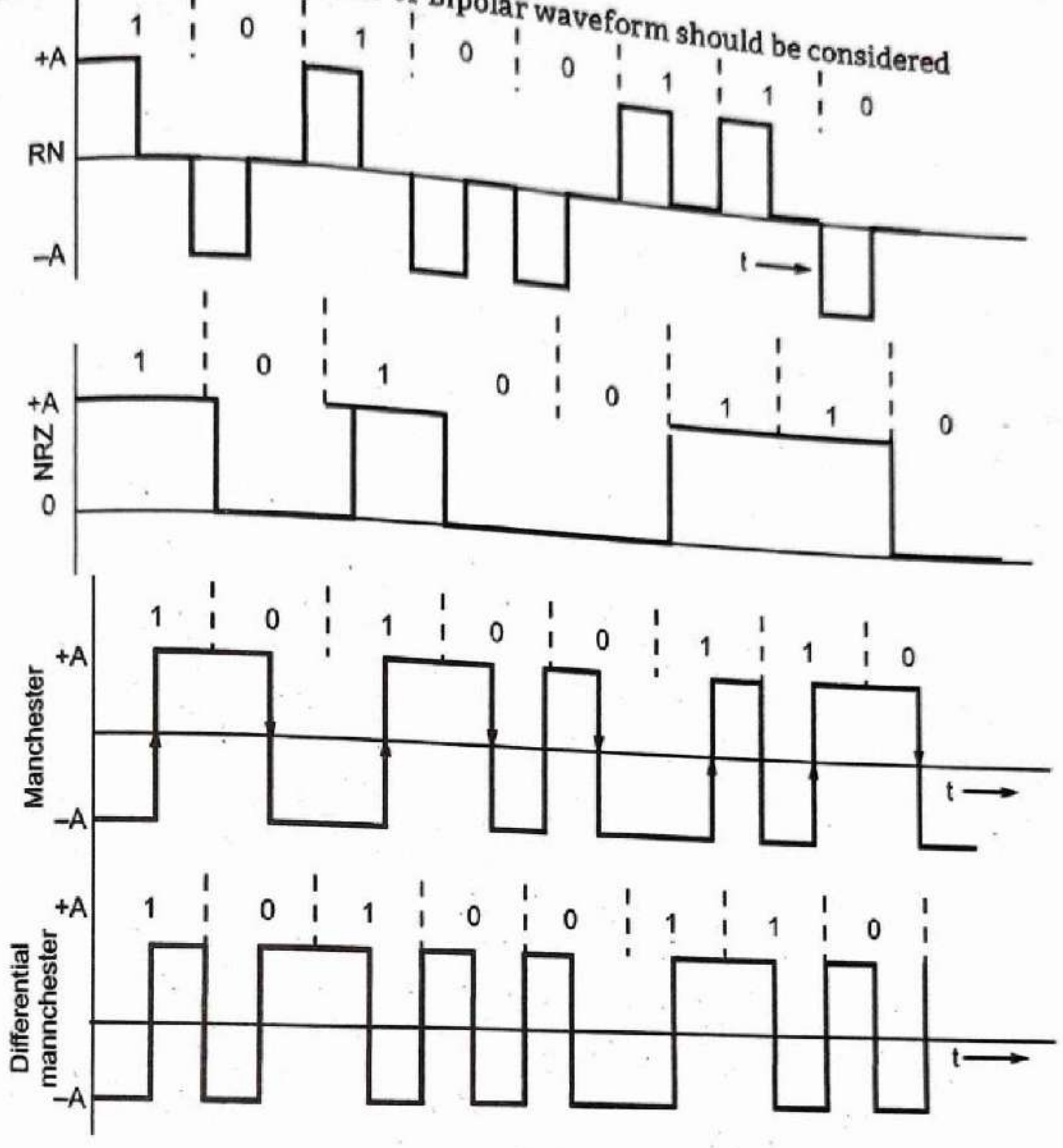


Fig. 4.3

4.4 AMPLITUDE SHIFT KEYING MODULATION

Amplitude Shift Keying (ASK) is the digital modulation technique in which the amplitude of the sinusoidal carrier will take one of the two predetermined values in response to 0 or 1 value of the digital input modulating message signal.

Amplitude shift keying is the simplest form of digital modulation. Here the carrier is a sine wave of frequency.

The digital signal from the information source is a unipolar NRZ signal which acts as the modulating signal. The ASK modulator is nothing but a multiplier followed by a band pass filter as shown in above Fig. 4.4 (a).

Due to multiplication, the ASK output will be present only when a binary „1 is to be transmitted and when the digital input is „0 then we get zero output as shown in the waveform above Fig. 4.4 (b).

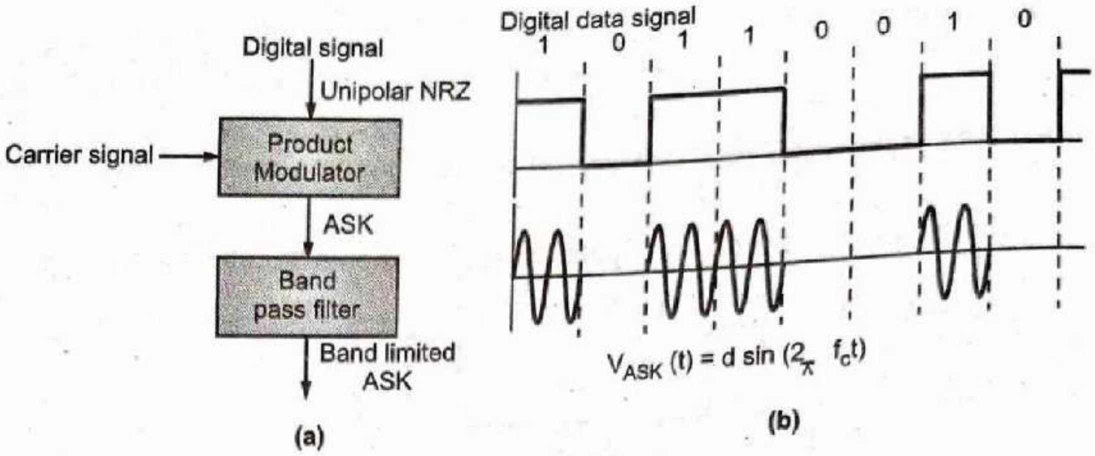


Fig. 4.4 : ASK

- From the waveform analysis we can conclude that when a binary „1 is to be sent the carrier is transmitted and when binary „0 is to be sent then the carrier is not transmitted.

4.4.1 BPSK Generator With Block Diagram and Waveforms

- BPSK stands for Binary phase shift keying. The digital information from the source may be a unipolar NRZ data which varies between values 1 and 0.
- But if digital data is unipolar then during 0 data output will be zero due to use of multipliers at transmitter. So to avoid this problem the unipolar data is first converted into bipolar data whose value varies between + 1 and – 1.
- The transmitter of BPSK signal is shown in the above Fig. 4.5.

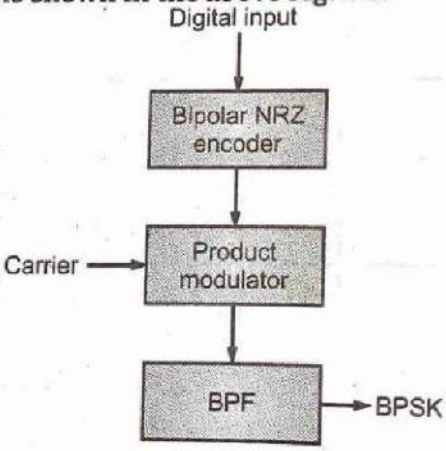


Fig. 4.5: BPSK

- The digital signal from the information source is a unipolar NRZ signal which is first converted into bipolar signal. This signal acts as the modulating signal. The BPSK modulator is nothing but a multiplier followed by a band pass filter as shown in above Fig. 4.5.
- Due to multiplication, the BPSK output will be present with 0° phase shift when a binary '1' is to be transmitted and when the digital input is '0' then we get BPSK output with 180° phase shift as shown in the waveform Fig. 4.6.
- From the waveform analysis we can conclude that when a binary '1' is to be sent the carrier is transmitted with 0° phase shift and when binary '0' is to be sent then the carrier is transmitted with 180° phase shift.
- The transmitted BPSK signal is $s(t) = b(t)\sqrt{2Ps}\cos\omega_0 t$.

- The phase of this signal changes depending on the time delay from transmitter to receiver. This phase change is generally fixed in the transmitted signal. Let the phase shift be θ.
- Therefore the signal at the input pf receiver is $s(t) = b(t)\sqrt{2Ps}\ \cos \omega_0 t + \theta$.

Waveforms:

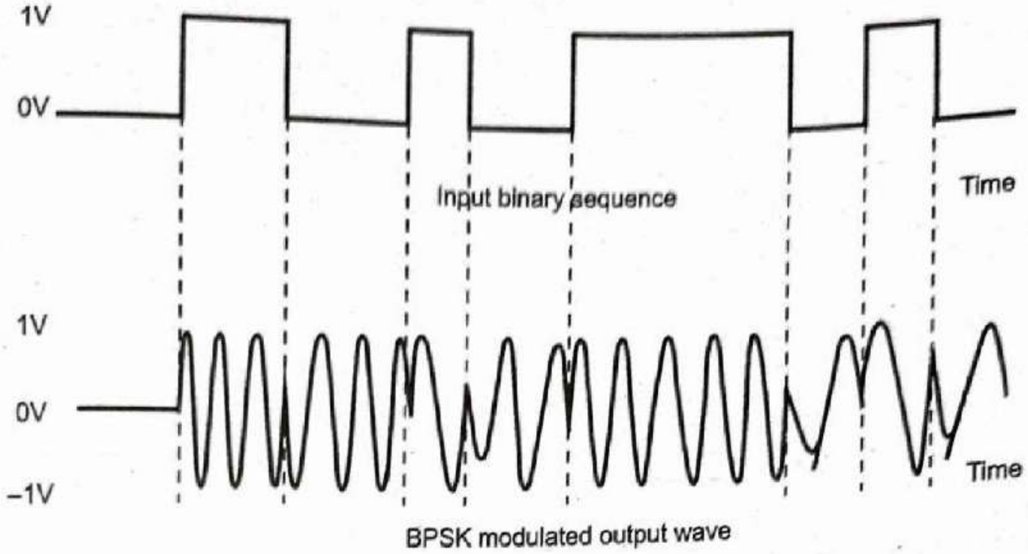


Fig. 4.6 : BPSK Waveforms

4.4.2 Block Diagram of PCM Transmitter and Receiver

- PCM stands for Pulse code Modulation.

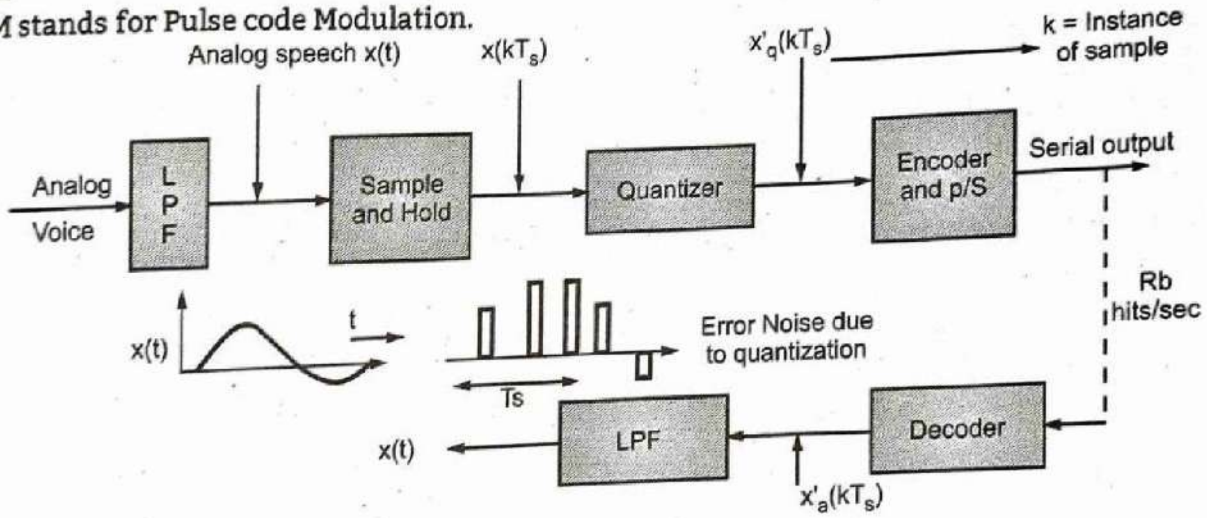


Fig. 4.7 : Schematic diagram of a PCM coder – decoder

- The technique in detail with block diagram as described below:
- The signal is band limited by the low pass filter.
- Let X(t) denote the filtered signal to be coded. The process of analog to digital conversion primarily involves three operations:
  1. Sampling of X(t),
  2. Quantization (i.e. approximation) of the discrete time samples, X (kT_s) and
  3. Suitable encoding of the quantized time samples $X_q(kT_s)$.
- Ts indicates the sampling interval where $R_s = 1/T_s$ is the sampling rate (samples /sec).
- A standard sampling rate for speech signal, band limited to 3.4 kHz, is 8 Kilo-samples per second (T_s = 125μ sec), thus, obeying Nyquist's sampling theorem.

Encoding:

- Encoding is used to translate the Discrete set of sample values to more appropriate signal called Code. Suppose in binary code word 'n' bits are used, then we may represent 2^n. After coding binary signal is represented by train of pulses as NRZ , RZ unipolar or bipolar.

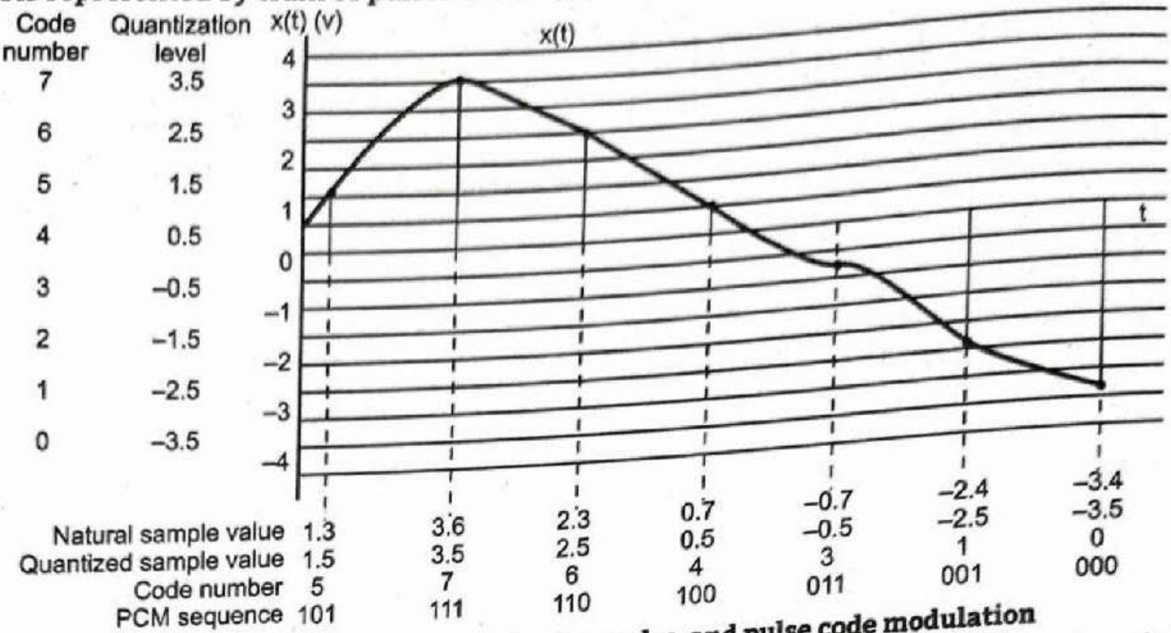
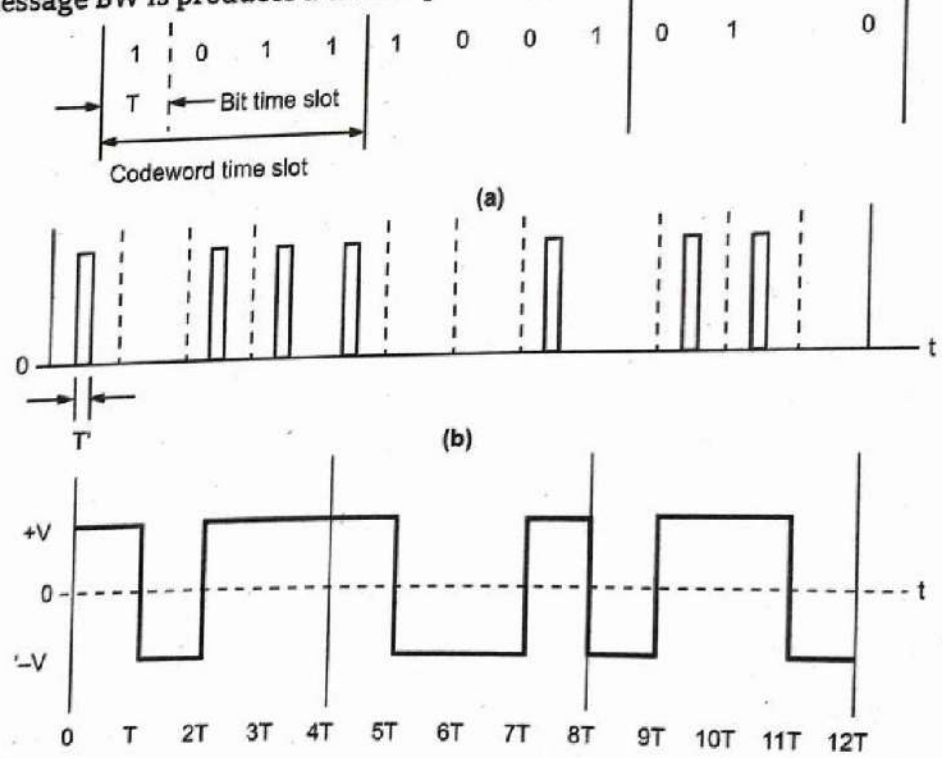


Fig. 4.8 : Natural samples, quantized samples, and pulse code modulation

- The PCM coded bit stream may be taken for further digital signal processing and modulation for the purpose of transmission.
- The PCM decoder at the receiver expects a serial or parallel bit-stream at its input so that it can decode the respective groups of bits (as per the encoding operation) to generate quantized sample sequence $[x'_q (kTs)]$.
- Following Nyquist's sampling theorem for band limited signals, the low pass reconstruction filter whose f_c = message BW is produces a close replica $\hat{x}(t)$ of the original speech signal x (t).



(a)

(b)

(c)

Fig. 4.9 : (a) PCM sequence. (b) Pulse representation of PCM (c) Pulse waveform(transition between two levels).

Multiplexing

- Different message sources are Time – Multiplexed for this receiver and transmitter are synchronized.

Channel Noise and Error Probability

- The Performance of PCM system is influenced by two major sources of Noice.
  1. Channel Noise : Introduced in transmission path
  2. Quantizing Noise : Introduced in transmitter

1. Channel Noise

Due to Channel Noise Symbol '0' appears as '1' and Vice versa.

Probability of error

$$P_e = 1/2 * \text{erfc}\,(1/2*(E_{max}/N_o)^{1/2})$$

Where No is noise power.

Quantizing Noise

Is produced at transmitter of PCM by rounding off analog sample value to nearby permissible level.

Quantizing Noise

$$\sigma^2_Q = \Delta^2 / 12$$

Where Δ is step size

Characteristics of PCM

1. Average Probability of error depends on ratio of Peak Signal energy to Noise spectral energy.
2. In PCM signal is regenerated so effects of amplitude , phase and nonlinear effects in one link has no effect on next link.
3. Transmission requirement PCM link are independent of total length of system.
4. PCM is very rugged system , means less noise effect unless noise amplitude is greater than half of pulse height.

Advantages

1. In PCM signal is regenerated so effects of amplitude, phase and nonlinear effects in one link has no effect on next link.
2. Transmission requirement PCM link are independent of total length of system.

Disadvantages:

1. High bit rate and noise limits the use.

Model Waveforms:

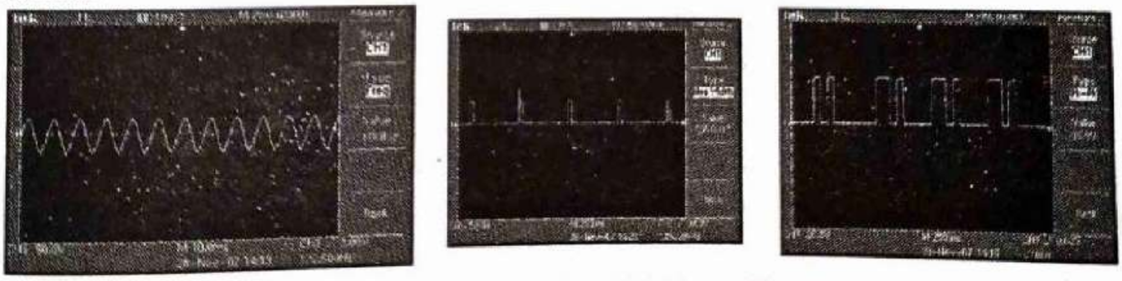


Fig. 4.10 : Waveforms of (a) Modulating Signal (b) Sampling Signal (c) PCM output

4.4.3 DPCM Transmitter and Receiver

- DPCM stands for Differential Pulse Code Modulation. The technique with block diagram is shown in Fig. 4.11.

- In PCM Samples of signal are usually correlated as amplitude of signal does not change much i.e. signal is correlated or carries redundant information. This aspect of speech signal is exploited in Differential Pulse Code Modulation (DPCM) technique.
- that a predictor block, a summing unit and a subtraction unit have been strategically added to the chain of blocks of PCM coder instead of feeding the sampler output x (kTs) directly to a linear quantizer. An error sample ep (kTs) is fed.

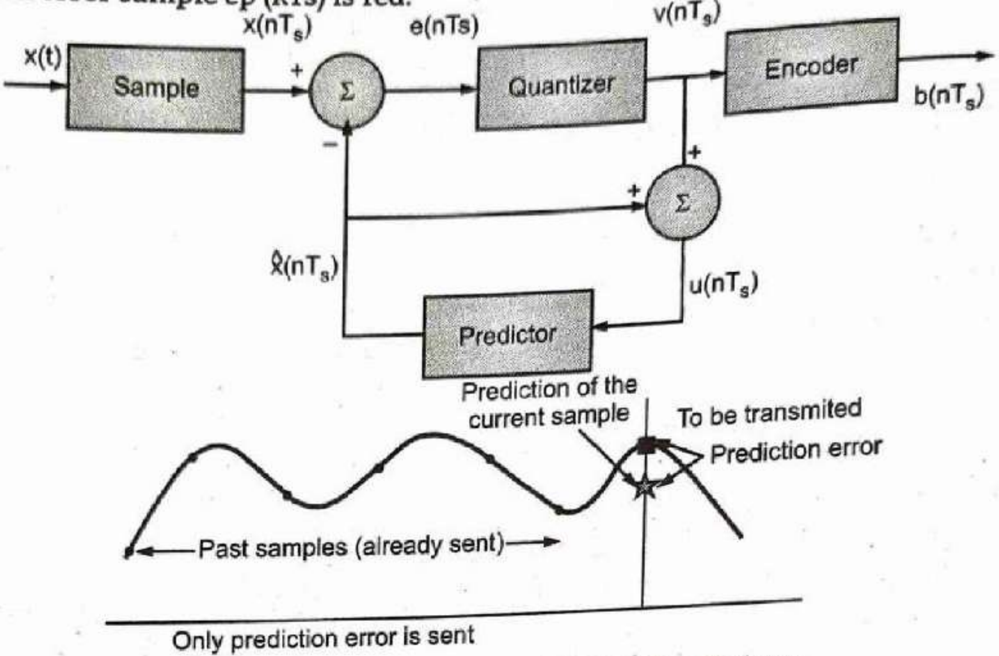


Fig. 4.11 : Schematic diagram of a DPCM modulator

- The error sample is given by the following expression:

$$e_p (nT_s) = x (nT_s) - x^\wedge (nT_s)$$

x^ (nT$_s$) is a predicted value for **x (nT$_s$)** and is supposed to be close to **x (nT$_s$)** such that **e_p (nTs)** is very small in magnitude **e_p (nTs)** is called as the 'prediction error for the nth sample'.

- We envisage smaller step size for the linear quantizer compared to the step size of an equivalent PCM quantizer. As a result, it should be possible to achieve higher SQNR for DPCM codec delivering bits at the same rate as that of a PCM codec.
- There is another possibility of decreasing the coded bit rate compared to a PCM system if an SQNR as achievable by a PCM codec with linear equalizer is sufficient.
- A block schematic diagram of a DPCM demodulator is shown in Fig. 4.12. The scheme is straightforward and it tries to estimate u(kT$_s$) using a predictor unit identical to the one used in the modulator.
- We have already observed that u(kT$_s$) is very close to x(kT$_s$) within a small quantization error of q(kT$_s$). The analog speech signal is obtained by passing the u^(kT$_s$)through an appropriate low pass filter.

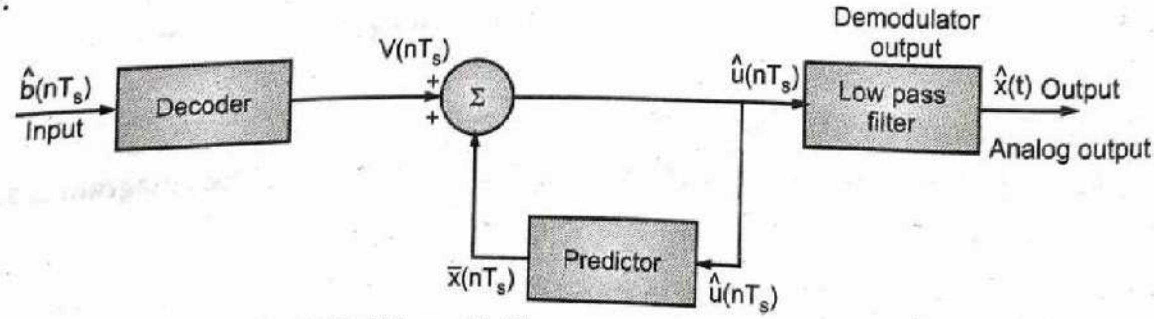


Fig. 4.12 : Schematic diagram of a DPCM demodulator

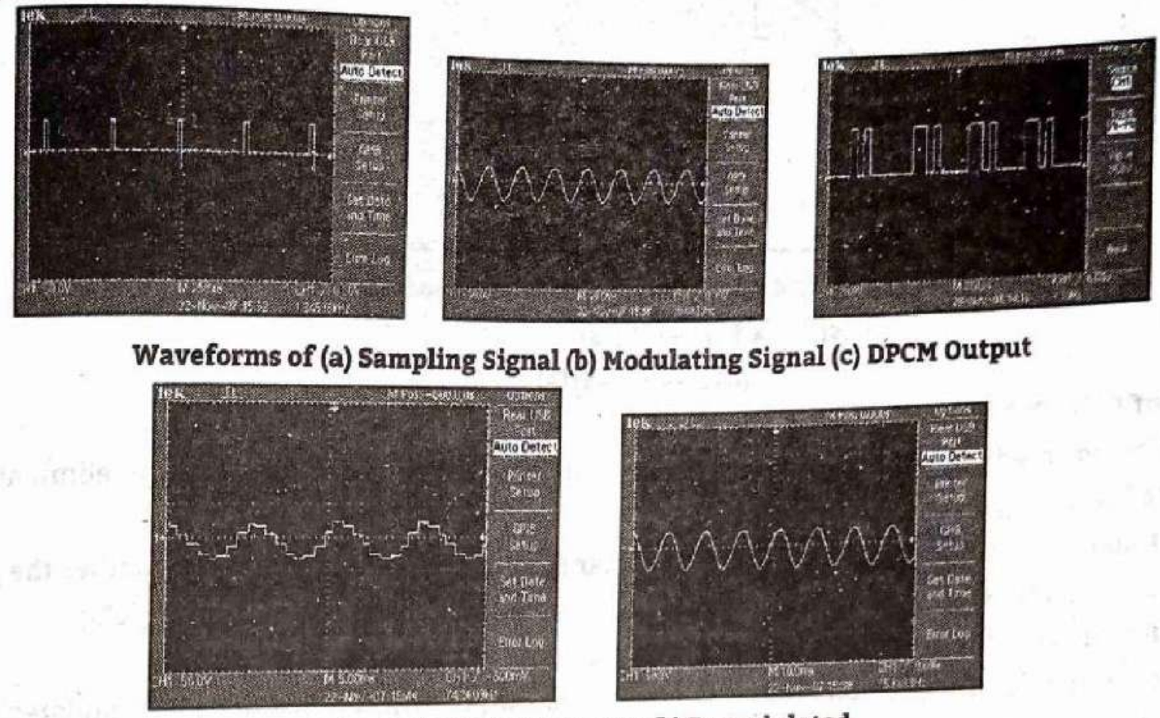
Advantages

1. Less bit rate generated so better utilization of bandwidth.
2. Redundant information is less carried

Disadvantages

1. Predicator increase hardware complexity of system.

Model Waveforms:



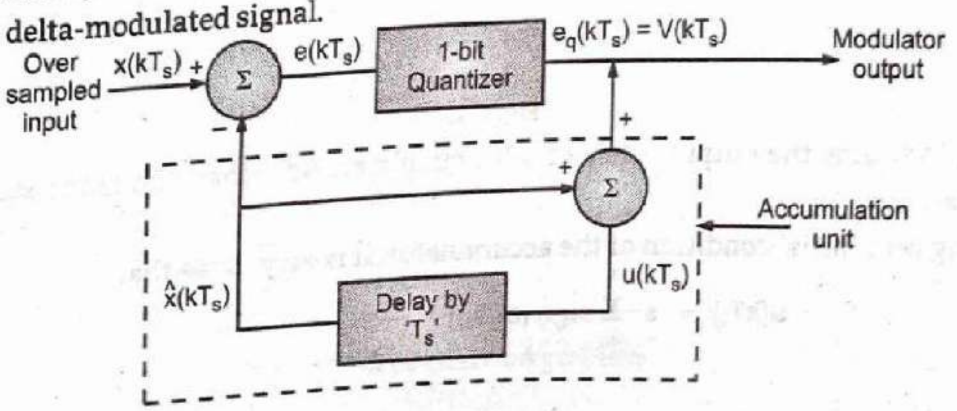
Waveforms of (a) Sampling Signal (b) Modulating Signal (c) DPCM Output

Output of (a) D/A Converter (b) Demodulated

Fig. 4.13: Waveforms

4.4.4 Block Diagram of Delta Modulation

- DM stands for Delta Modulation. The technique in detail as described below and shown in Fig. 4.14.
- If the sampling interval 'Ts' in DPCM is reduced considerably, i.e. if we sample a band limited signal at a rate much faster than the Nyquist sampling rate, the adjacent samples should have higher correlation.
- The sample-to-sample amplitude difference will usually be very small. So, one may even think of only 1-bit quantization of the difference signal. The principle of Delta Modulation (DM) is based on this premise.
- Delta modulation is also viewed as a 1-bit DPCM scheme. The 1-bit quantizer is equivalent to a two-level comparator (also called as a hard limiter). Fig. 4.14 shows the schematic arrangement for generating a delta-modulated signal.



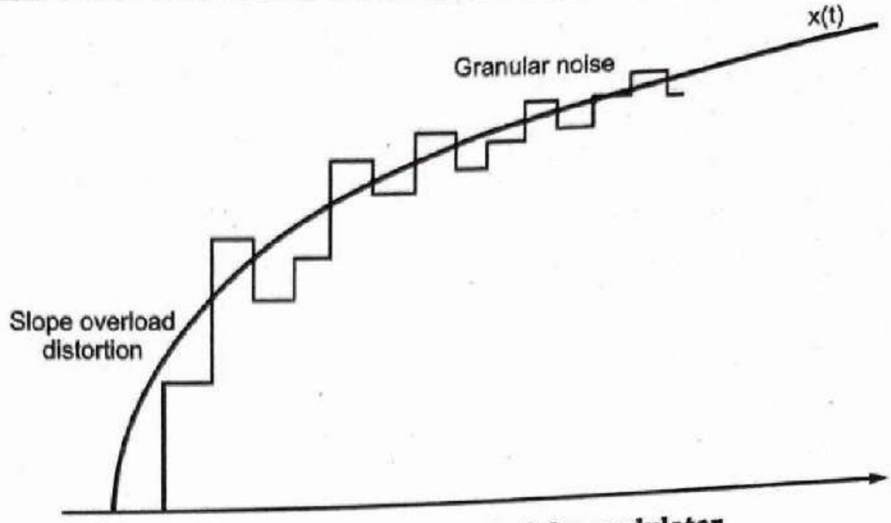


Fig. 4.14 :Block diagram of a delta modulator

Note that, $e(kTs) = x(kTs) - x\hat{}(kTs)$

$= x(kTs) - u([k-1]Ts)$

Features of Delta Modulation

- No effective prediction unit – the prediction unit of a DPCM coder (Fig. 4.14) is eliminated and replaced by a single-unit delay element.
- A 1-bit quantizer with two levels is used. The quantizer output simply indicates whether the present input sample x(kTs) is more or less compared to its accumulated approximation x^(kTs)
- Output x^(kTs) of the delay unit changes in small steps.
- The accumulator unit goes on adding the quantizer output with the previous accumulated version x^(kTs) . u(kTs), is an approximate version of x(kTs).
- Performance of the Delta Modulation scheme is dependent on the sampling rate.
- Most of the above comments are acceptable only when two consecutive input samples are very close to each other.

$$e(KT_s) = x(kT_s) - \{\hat{x}([k-1]T_s) + v([k-1]T_s)\}$$

further, $v(kT_s) = e_q(kT_s) = s.\text{sign}[e(kT_s)]$

Here, 's' is half of the step-size δ as indicated in Fig below

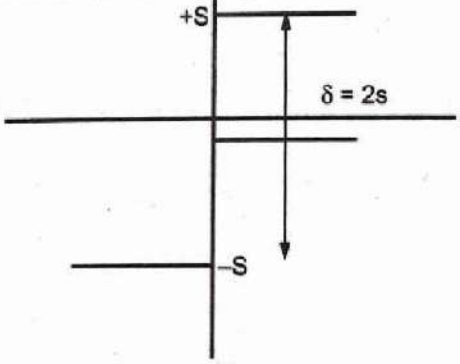


Fig. 4.15

- This diagram indicates the output levels of 1-bit quantizer. Note that of δ is the step size, the two output levels are ± s
- Now, assuming zero initial condition of the accumulator, it is easy to see that

$$u(kT_s) = s \cdot \sum_{j=1}^{k} \text{sign}\,[e(jT_s)]$$

$$u(kT_s) = \sum_{j=1}^{k} v(jT_s)$$

Further, $$\hat{x}(kT_s) = u([k-1]T_s) = \sum_{j=1}^{k-1} v(jT_s)$$

- Above eq. shows that is essentially an accumulated version of the quantizer output for the error signal e^(kt$_s$)- x^(kt$_s$) . also gives a clue to the demodulator structure for DM.
- Fig. 4.16 shows a scheme for demodulation.

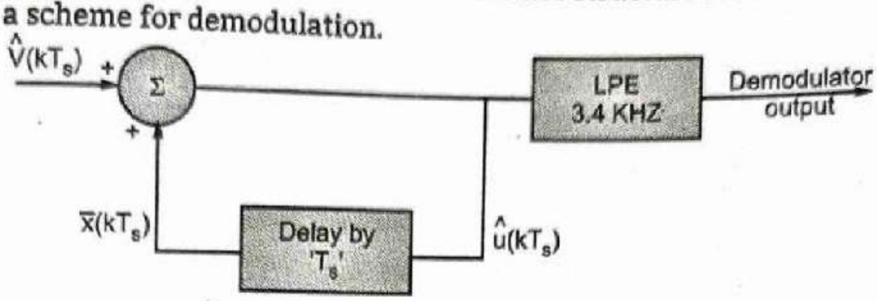


Fig. 4.16 : Demodulator structure for DM

- The input to the demodulator is a binary sequence and the demodulator normally starts with no prior information about the incoming sequence.
- Now, let us recollect from our discussion on DPCM in the previous lesson that, u(kTs) closely represents the input signal with small quantization error q(kTs), i.e.

$$u(kT_s) = x(kT_s) + e(kT_s)$$

- Next, from the close loop including the delay-element in the accumulation unit in the Delta modulator structure, we can write

$$u([k-1]T_s) = \hat{x}(kT_s) = x(kT_s) - e(kT_s) = x([k-1]T_s) + q([k-1]T_s)$$

Hence, we may express the error signal as,

$$u(kT_s) = \{x(kT_s) - x([k-1]T_s)\} - q([k-1]T_s)$$

That is, the error signal is the difference of two consecutive samples at the input except the quantization error (when quantization error is small).

Advantages of a Delta Modulator over DPCM

1. As one sample of x(kTs) is represented by only one bit after delta modulation, no elaborate word-level synchronization is necessary at the input of the demodulator. This reduces hardware complexity compared to a PCM or DPCM demodulator.
2. Bit-timing synchronization is, however, necessary if the demodulator in implemented digitally.
3. Overall complexity of a delta modulator-demodulator is less compared to DPCM as the predictor unit is absent in DM.

Limitations of DM:

1. **Slope Over Load Distortion:** If the input signal amplitude changes fast, the step by step accumulation process may not catch up with the rate of change as shown in Fig. 4.17.

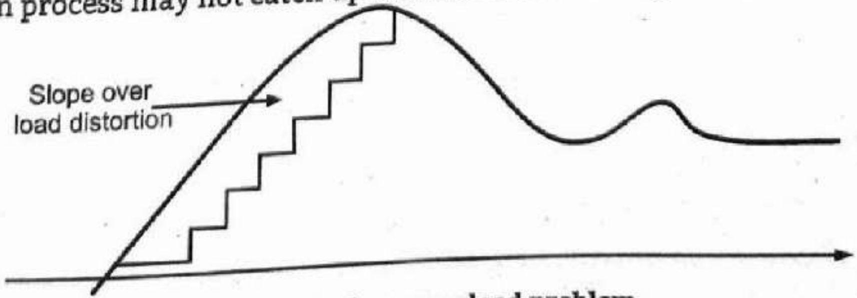


Fig. 4.17: slope-overload problem

An intuitive remedy for this problem is to increase the step-size δ but that approach has another serious problem given below.

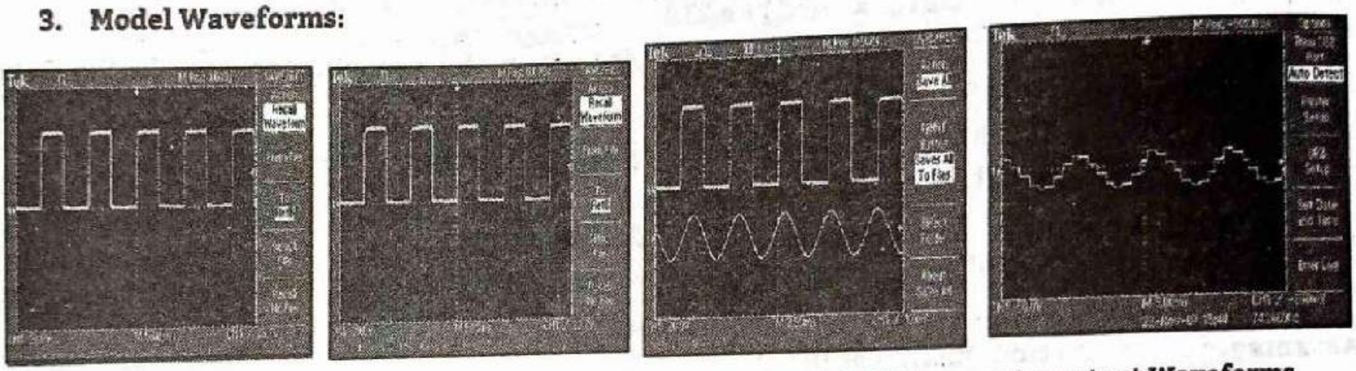
2. **Granular Noise:**

If the step-size is made arbitrarily large to avoid slope-overload distortion, it may lead to 'granular noise'. Imagine that the input speech signal is fluctuating but very close to zero over limited time duration. This may happen due to pauses between sentences or else. During such moments, our delta modulator is likely to produce a fairly long sequence of 101010...., reflecting that the accumulator output is close but alternating around the input signal. This phenomenon is manifested at the output of the delta demodulator as a small but perceptible noisy background. This is known as 'granular noise'. A more efficient approach of adapting the step-size, leading to **Adaptive Delta Modulation** (ADM), Condition for avoiding slope overload:

We may observe that if an input signal changes more than half of the step size (i.e. by 's') within a sampling interval, there will be slope-overload distortion. So, the desired limiting condition on the input signal x(t) for avoiding slope-overloading is,

$$\frac{dx(t)}{dt}\Bigg|_{\max} \le \frac{s}{T_s}$$

3. **Model Waveforms:**



(a) Clock input (b) Delta modulation output and message signal (c) D/A converter output Waveforms

Fig. 4.18 : Waveforms

4.4.5 Slope Overload and Granular Noise with Respect to Delta Modulation

Fig. 4.19 : Graph showing Slope overload and Granular noise

- The delta modulation has two major drawbacks as under:

1. **Slope Overload Distortion**

- This distortion is arises because of large dynamic range of the input signal. As can be observed from figure the rate of rise of input signal x(t) is so high that the staircase signal cannot approximate it, the steep size „Δ" becomes too small for staircase signal x"(t)to follow the step segment of x(t).
- Hence, there is a large error between the staircase approximated signal and the original input signal x (t). This error or noise is known as slope overload distortion. To reduce this error, the step size must be increased when slope of signal x (t) is high.
- Since the step size of delta modulator remains fixed, its maximum or minimum slopes occur along straight lines. Therefore, this modulator is also known as Linear Delta Modulator (LDM).

2. **Granular or Idle Noise:**

- Granular or Idle noise occurs when the step size is too large compared to small variations in the input signal. This means that for very small variations in the input signal, the staircase signal is changed by large amount (Δ) because of large step size figure shows that when the input signal is almost flat, the staircase signal x"(t) keeps on oscillating by ±Δ around the signal.
- The error between the input and approximated signal is called granular noise. The solution to this problem is to make step size small.
- Therefore, a large step size is required to accommodate wide dynamic range of the input signal (to reduce slope overload distortion) and small steps are required to reduce granular noise. In fact, Adaptive delta modulation is the modification to overcome these errors.

4.4.6 Comparison in PCM, DPCM and DM

Table 4.3

Characteristics	PCM	DPCM	DM
Principle	Each discrete sample is quantized, encoded and sent.	Difference between consecutive samples is quantized, encoded and sent.	Sampling rate > Nyquist sampling rate so ample-to-sample amplitude difference is very low about 1-bit quantization which is encoded and send
Redundant Information	Carries redundant information.	Carries Less redundant information.	Carries high redundant information than PCM.
Bit rate generated	Higher compare to DPCM	Very Low compare to PCM	Higher than PCM
No. of Quantization levels.	High compare to DPCM, DM	Less compare to PCM	Less compare to DPCM, PCM
Quantization Noise	High compare to DPCM	Less compare to PCM, DM	High compared to PCM , DPCM due to step size called as Slope overload error and Granular Noise
Predictor Requirement	No	Yes	No, instead single Delay element is used.

Contd. ...

Advantages	In PCM signal is regenerated so effects of amplitude, phase and nonlinear effects in one link has no effect on next link.	Less bit rate generated so better utilization of bandwidth.	Due to one bit quantization, no elaborate word-level synchronization is necessary at the input of the demodulator. This reduces hardware complexity compared to a PCM or DPCM demodulator.
	Transmission requirement PCM link are independent of total length of system.	Redundant information is less carried	Overall complexity of a delta modulator-demodulator is less compared to DPCM as the predictor unit is absent in DM.
Disadvantages	High bit rate and noise limits use	Predicator increase hardware complexity of system.	Higher Quantization noise compared to PCM , DPCM
Application	Telephone Speech	Video Chatting	Video streaming

4.4.7 Spread Spectrum Signal Different from Normal Signal

- This signal occupies a larger bandwidth than that of normal signal. The spread spectrum signal invariably uses some kind of coding.
- The spectrum spreading at the transmitter and dispreading at the receiver is obtained with the help of this code word. The code word associated with an ss signal is independent of the information carried by the signal.
- The most important point is that ss signal is pseudorandom in nature.This makes it appear like random noise. Hence the normal receiver cannot demodulate ss signal. Only a specially designed receiver can demodulate it to recover the information

Advantages of Spread Spectrum:

1. Low power density
2. Redundancy
3. Anti-jamming
4. Anti-interference
5. Low probability of intercept
6. Message privacy
7. High resolution raging and timing

Disadvantages of Spread Spectrum :

1. Large amount of bandwidth is rewired

Applications of Spread Spectrum :

1. Military application-resistance to gaining
2. Secure communication

3. CDMA in satellite communication
4. Police radar can employ spread spectrum to avoid detection by detectors employed by drives
5. Low density power spectra for signal hiding
6. LAN
7. GPS
8. Multipath rejection in ground based mobile station.

4.4.8 Direct Sequence Spread Spectrum (DSSS)

- Direct Sequence Spread Spectrum (DSSS): In direct sequence, the serial binary data is mixed with a higher frequency pseudorandom binary code at a faster rate and the result is used to phase-modulate a carrier. Direct Sequence Spread Spectrum Coherent PSK Transmitter
- The averaging system reduces the interference by averaging at over a long period the DSSS system is a averaging system. This technique can be used in practice for transmission of signal over a band pass channel (e.g. satellite channel). For such application the coherent Binary Phase Shift (BPSK) is used in the transmitter and receiver.

Transmitter: Fig. 4.20 shows DSSS transmitter.

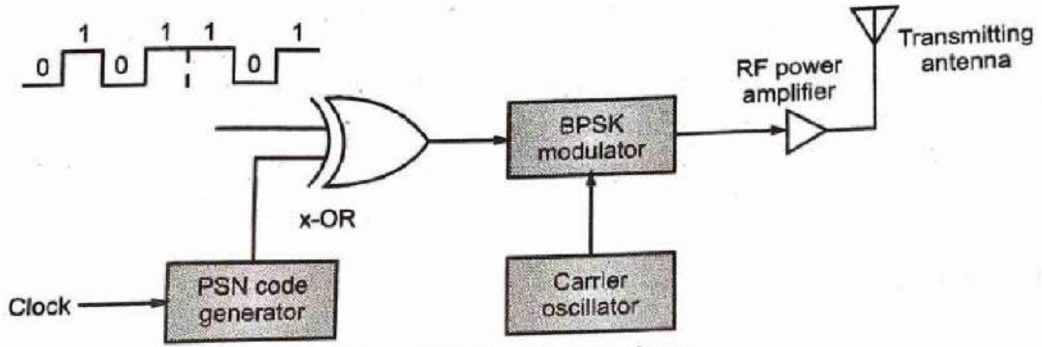


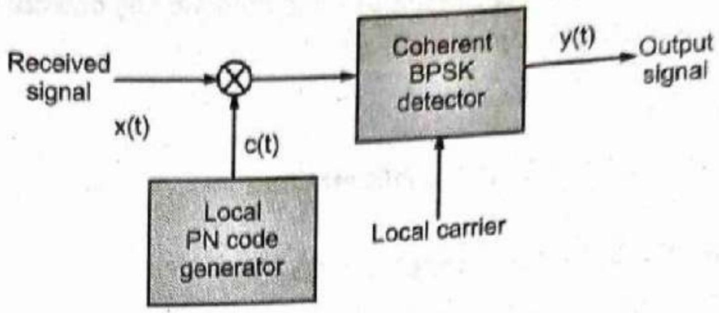
Fig. 4.20 : DSSS Transmitter

Explanation:

- The block diagram of DSSS transmitter is shown in Fig. 4.20. The serial binary data is applied to an X-OR gate along with a serial pseudorandom code that occurs faster than binary data.
- The signal developed at the output of the X-OR gate is then applied to a BPSK modulator. The carrier phase is switched between 0°and 180° by the 1"s and 0"s of X –OR output.
- The signal phase modulating carrier, being much higher in frequency than the data signal causes the modulator to produce multiple widely spaced sidebands whose strength is such that the complete signal takes up a great deal of the spectrum. Thus the signal is spread. Also because of its randomness, the resulting signal is appears to be nothing more than wideband noise to a conventional narrow band receiver.
- One bit time for the pseudorandom code is called a chip and the rate of the code is called the chipping rate. The chipping rate is faster than the data rate.
- The receiver signal X(t) and the locally generated replica of the PN sequence generator are applied to a multiplier this is 1st stage of multiplication. The multiplier performs the de-spreading operation output of multiplier is then applied to a coherent BPSK detector with local carrier applied to it.

- At the output of coherent BPSK detector we get back the original signal d(t) data signal.

Receiver:



The DS-BPSK receiver

(OR)

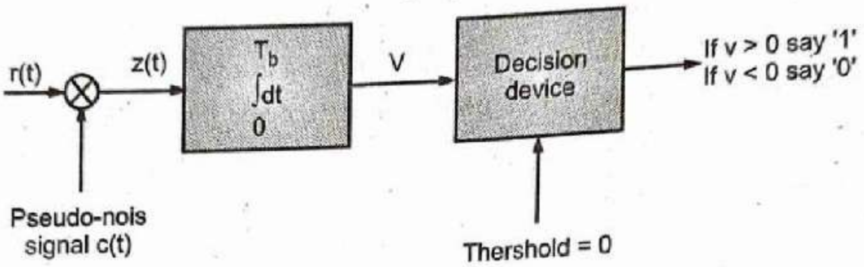


Fig. 4.21 : DSSS Receiver

Features of DSSS:

1. It provides good security against potential jamming or interpretation
2. The DSSS is extremely effective against narrowband jamming signal
3. The narrowband communication signal can coexist with DSSS signal
4. The DSSS signal is not very effective against broadband interference.

Disadvantages of DSSS:

1. With the serial search system, the acquisition time is too large. This makes DSSS system slow
2. The sequence generated at the PN code generator output must have high rate. The length of such sequence needs to be long enough to make the sequence truly random
3. The channel bandwidth required is very large, But this bandwidth is less than that of FHSS system
4. The synchronization is affected by the variable distance between the transmitter and receiver

Applications of DSSS System:

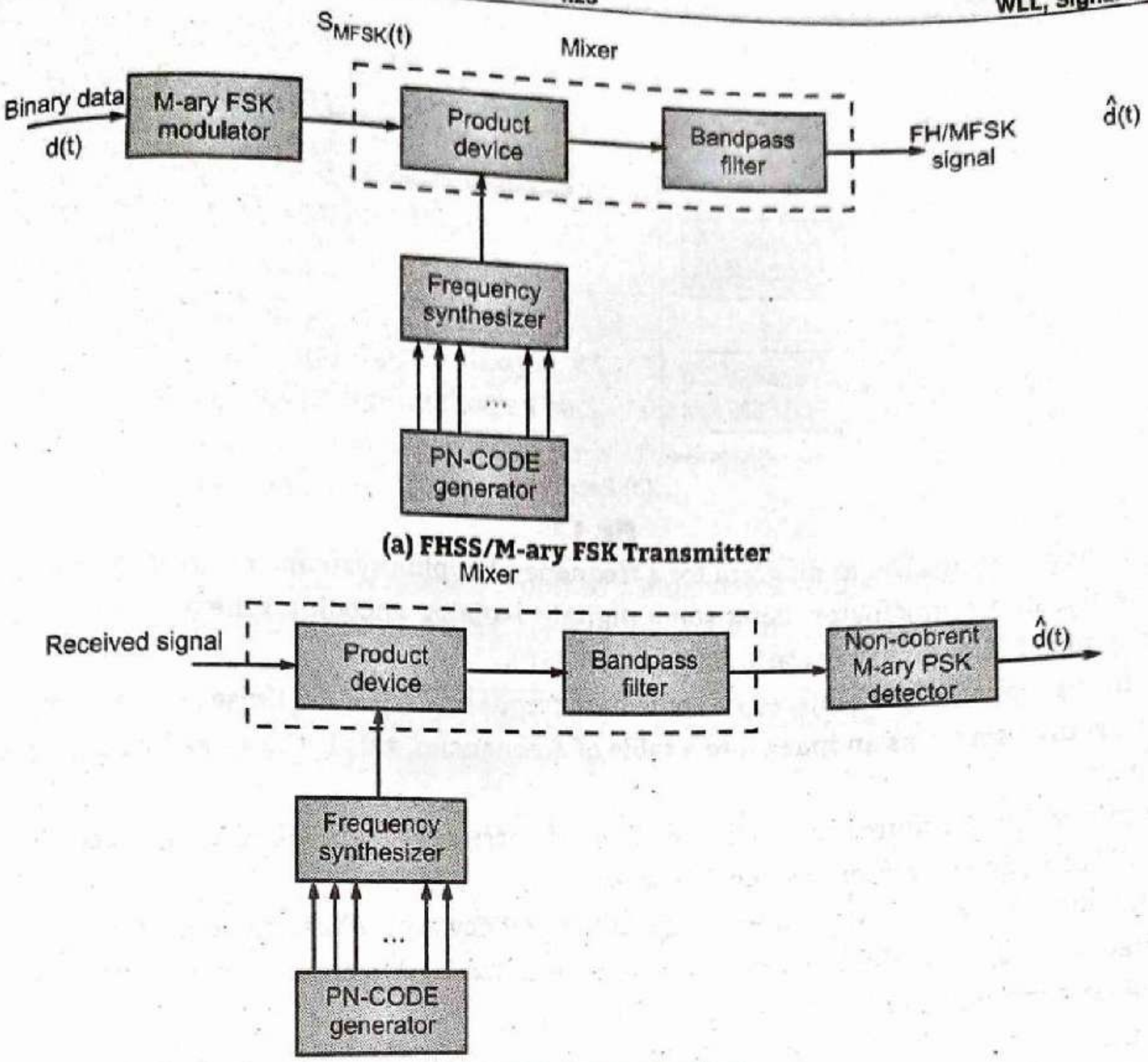
1. To compact intentional interference
2. To reject unintentional interference
3. To minimize self interference due to multipath propogation
4. In the low probability of intercept signal
5. In obtaining message privacy
6. code division multiple access with DSSS

4.4.9 Frequency Hopping Spread Spectrum (DSSS)

- FHSS stands for Frequency hoping spread spectrum modulation.

Different Types Of Frequency Hoping (Slow and fast frequency hoping).

- FHSS combines spread spectrum modulation with MFSK. It is the process of Modifying Frequency of MFSK Signal using frequency hope generated by bits of PN sequence

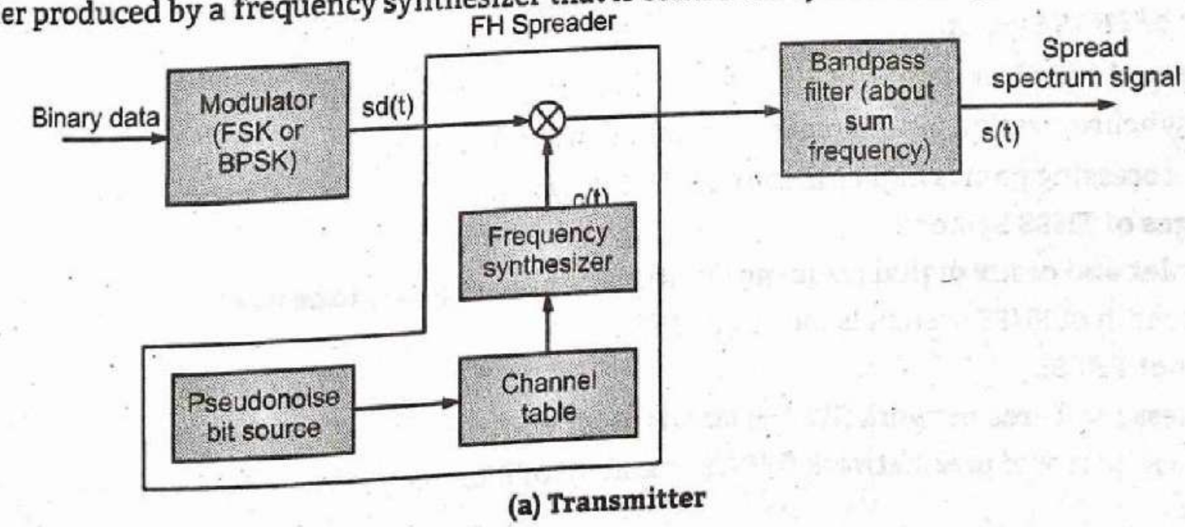


(a) FHSS/M-ary FSK Transmitter

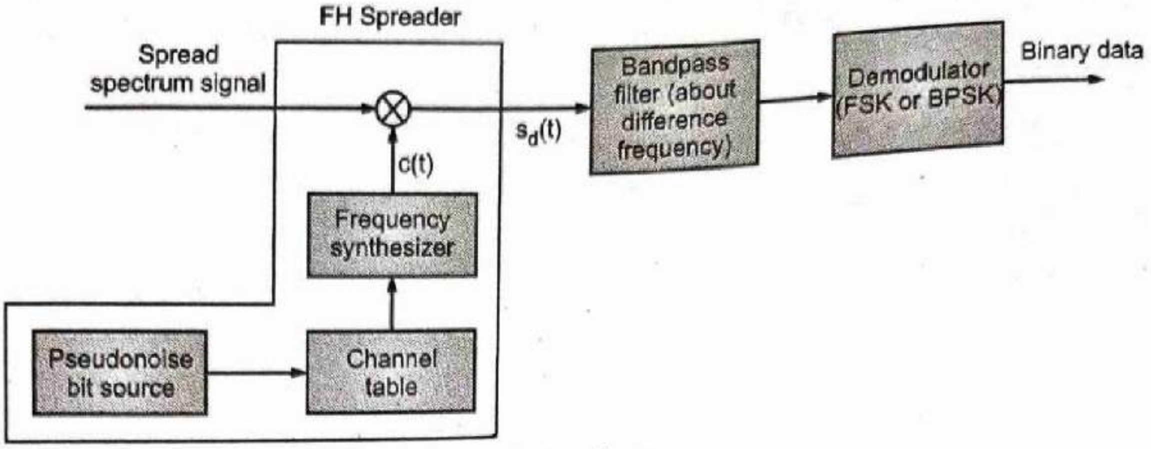
(b) FHSS/M-ary FSK Receiver

Fig. 4.22 : FHSS Transmitter and Receiver

- The binary digital data modulates a carrier using a traditional modulation scheme like M-ary FSK.
- This M-ary FSK modulated signal is then modulated a second time by another carrier frequency, but this carrier frequency changes its value, or rather hops, at regular intervals of T_c, the chip period, from one value to another form among a given set of values, accordingly to a pre-determined, pseudo-random pattern. This carrier frequency hopping is controlled at the transmitter by a pseudo-random code generator, as shown in Fig. 4.23.
- The binary data is first used to produce an M-ary FSK modulated signal. This is again modulated by a carrier produced by a frequency synthesizer that is controlled by a PN code generator.



(a) Transmitter



(b) Receiver

Fig. 4.23

- Fig. 4.23 shows a typical block diagram for a frequency-hopping system.For transmission, binary data are fed into a modulator using some digital-to-analog encoding scheme, such as Frequency Shift Keying (FSK) or Binary Phase Shift Keying (BPSK).
- The resulting signal $s_d(t)$ is centered on some base frequency. A Pseudo Noise (PN), or pseudorandom number, source serves as an index into a table of frequencies; this is the spreading code referred to previously.
- Each k bits of the PN source specifies one of the 2^k carrier frequencies. At each successive interval (each k PN bits), a new carrier frequency is selected.
- The frequency synthesizer generates a constant-frequency tone whose frequency hops among a set of 2^k frequencies, with the hopping pattern determined by k bits from the PN sequence. This is known as the spreading or **chipping signal** c(t).
- This is then modulated by the signal produced from the initial modulator to produce a new signal with the same shape but now centered on the selected carrier frequency.
- A bandpass filter is used to block the difference frequency and pass the sum frequency, yielding the final FHSS signal s(t).
- On reception, the spread spectrum signal is demodulated using the same sequence of PN-derived frequencies and then demodulated to produce the output data.
- At the receiver, a signal of the form s(t) defined on the previous slide, will be received. This is multiplied by a replica of the spreading signal to yield a product signal.
- A bandpass filter is used to block the sum frequency and pass the difference frequency, which is then demodulated to recover the binary data.

Advantages of FHSS System:

1. The serial search system with FHSS needs shorter time for acquisition.
2. The synchronization is not greatly dependent on the distance.
3. The processing gain is higher than that of DSSS system.

Disadvantages of FHSS System:

1. Complex and costly digital frequency synthesizers are required to be used.
2. Bandwidth of FHSS system is too large (GHZ).

Applications of FHSS:

1. Wireless local area network (WLAN) standard for wi-fi.
2. Wireless personal area network (WPAN) standard of Bluetooth.

Comparison of FHSS and DSSS System:

Table 4.4

DSSS	FHSS
Definition: PN sequence of large bandwidth is multiplied with narrow band information signal	Definition: Data bits are transmitted in different frequency slots which are changed by PN sequence
chip rate = 1/TC	chip rate = max(Rh, Rs)
Application with large multipath delays: DS represents a reliable mitigation method as such signal render all multipath signal copies that are delayed by more than one chip time from direct signal as invisible to the receiver	FH system can provide the same mitigation only if the hopping rate is faster than symbol rate and if the hopping bandwidth is larger
For commercial applications implementation of DSSS radios with large gap can also be costly due to need of high speed circuits	Implementation of FHSS radio can be costly and complex due to need of high speed frequency synthesizers
DSSS radios encounter more randomly distributed error that are continuous and lower level	FHSS suffers from burst error
Modulation Technique : BPSK	Modulation Technique : M-ary FSK
Long acquisition Time	Short acquisition time
DSSS is distance dependent	In FHSS , ffect of distance is less
Processing gain is less	Processing gain is higher
Bandwidth required is less than FHSS system	Bandwidth of FHSS system is too high
Effect of fading is more	Effect of fading is less

Comparison of Slow Frequency and Fast Frequency Hopping:

Table 4.5

Slow Frequency Hopping	Fast Frequency Hopping
More than one symbols are transmitted per frequency hop.	More than one frequency hops are required to transmit one symbol.
Chip rate is equal to symbol rate.	Chip rate is equal to hop rate.
Symbol rate is higher than hop rate.	Hop rate is higher than symbol rate.
Same carrier frequency is used to transmit one or more symbols.	One symbol is transmitted over multiple carrier in different hops.
A jammer can detect this signal if the carrier frequency in one hop is known.	A jammer can not detect this signal because one symbol is transmitted using more than one carrier frequencies.

Practice Questions

1. Draw and explain WLL architecture in detail.
2. What are various WLL technologies?
3. What are different WLL types?
4. Compare CT-2,DECT,PHS?

5...

Mobile Ad-hoc Networks and Wireless Sensor Networks

Chapter Outcomes...

- Explain the feature of given component in MANET architecture.
- Explain characteristics of the given WSN architecture.
- Describe the given design challenges in WSN.
- Classify the given clustering algorithm.
- State the procedure of scheduled maintenance of the given system.

Learning Objectives...

- To understand Basic Concepts of Mobile Ad-hoc Networks
- To learn Wireless Sensor Network
- To study MANET and Mesh Networking
- To learn WSN and IoT

5.0 INTRODUCTION

- Advancement in the field of internet due to wireless networking gives rise to many new applications. Mobile Ad-hoc Network is one of the most promising fields for research and development of wireless network.
- As the popularity of mobile device and wireless networks has significantly increased over the past years, ad-hoc network has now become one of the most vibrant and active field of communications and networks.
- MANET is an autonomous collection of mobile devices (Laptops, smart phones, sensors etc) that communicate with each other over wireless links and co-operate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure.
- This type of network operating as a stand-alone network or multiple point of attachment to cellular networks or Internet paves the way for numerous new and exciting applications.
- A mobile ad hoc network (MANET) is a collection of mobile nodes that act as both routers and hosts in an ad hoc wireless network and that dynamically self-organize in a wireless network without using any pre-established infrastructure.
- Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

5.1 MANET

- A MANET is a collection of mobile nodes which are independent. Mobile nodes in MANET communicate to each other via radio waves.
- MANET is defined as is a type of Ad-hoc Network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. It is an autonomous system of mobile host connected by wireless link.
- In cellular network communication between two Mobile Hosts (MH) completely rely on the wired backbone and fixed base station but in MANET no such infrastructure exists and network topology may dynamically change in an unpredictable manner since nodes are free to move. Change in topology made known to other nodes so that outdated topology information can be updated or removed.
- Ad-hoc network are basically peer to peer multi-hop mobile wireless network, where information packets are transmitted in store and forward manner from source to arbitrary destination.

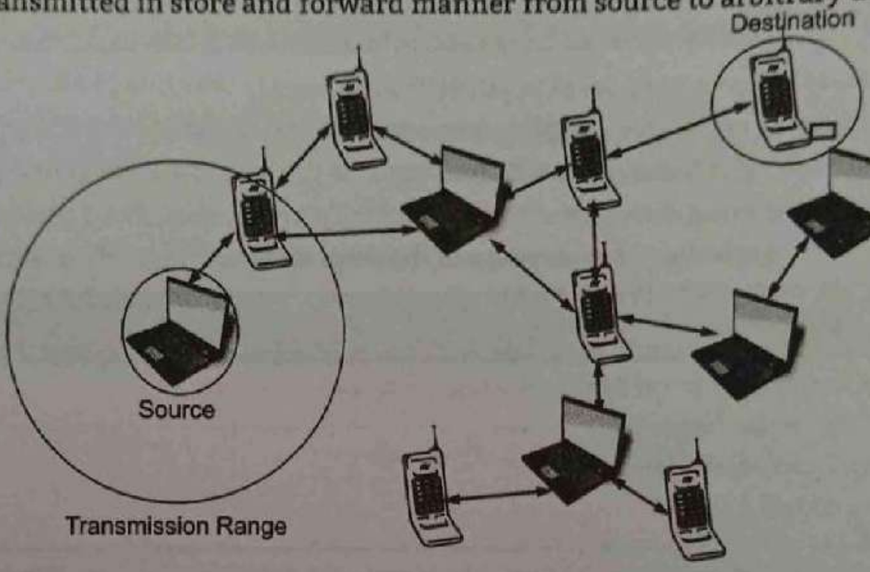


Fig. 5.1: MANET

5.1.1 MANET Topologies

- The dynamic collection of mobile nodes creating short-lived networks with the absence of mixed infrastructure is called as MANET.
- Every node in MANET has wireless transmitter and receiver with proper antenna. All nodes acts as routers connected by wireless links.
- Fig. 5.2 represents MANET topology.

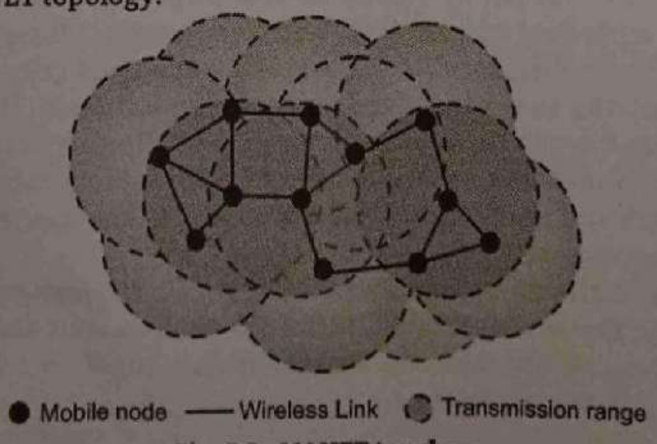


Fig. 5.2 : MANET topology

Topology Formation:

1. **Neighbour Discovery:**

- The performance of Ad-hoc Network depends on the interaction among communicating entities in a given neighbourhood.
- Thus, in general, before a node starts communicating, it must discover the set of nodes that are within its direct communication range. Once this information is gathered, the node keeps it in an internal data structure so that it can be used in different networking activities such as routing.
- The behaviour of an Ad-hoc node depends on the behaviour of its neighbouring nodes because it must sense the medium before it starts transmitting packets to the nodes in its interfering range, which can cause collision at the other nodes.
- Node discovery can be achieved with periodic transmission of beacon packets or with promiscuous snooping on the channel to detect the communication activity.

2. **Packet Forwarding Algorithms:**

- An important part of a routing protocol is the packet forwarding algorithm that chooses the one to be used to forward the data packet among neighbouring nodes.
- The forwarding algorithm implements a forwarding goal that may be, for instance, the shortest average hop distance from source to destination.
- In this case, the set of potential nodes may include only those in direct communication range from the current node or also the set of possible nodes in the route to the destination.
- The forwarding goal may also include some QoS parameters such as the amount of energy available at each node. The following forwarding algorithms consider only nodes that are in direct communication range of the node that has a data packet to be forwarded, as depicted in Fig 5.2.
- The Most Forward within Radius (MFR) forwarding algorithm chooses the node that maximises the distance from node S to point p. In this case, as depicted in Fig 5.2 it is node 1.
- Contrarily, the Nearest Forward Progress (NFP) forwarding algorithm chooses the node that minimises the distance from node S to point q. Here, it is node 2. The Greedy Routing Scheme (GRS) uses the nodes geographical location to choose the one that is very close to the destination node D. And here it is node 3.
- The Compass Selecting Routing (COMPASS) algorithm chooses the node that minimises the angle, but considers the nodes that are closer to node D. Hence, it is node 4. The random process forwarding algorithm, as the name suggest, chooses a random node that is in direct communication range from S.

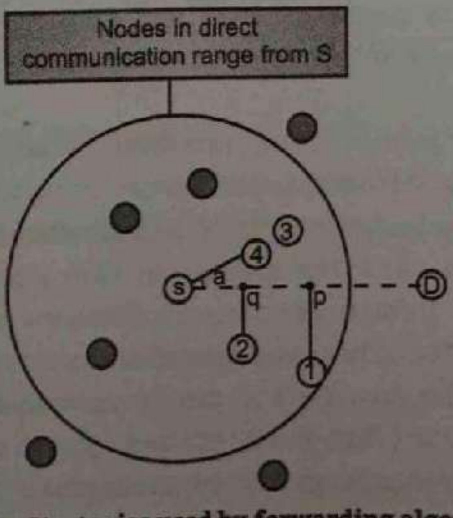


Fig. 5.3 : Strategies used by forwarding algorithms

- The Partial Topology Knowledge Forwarding (PTKF) algorithm chooses a node using a localised shortest path weighted routing where routes are calculated based on the local topological view and considering the transmission power needed to transmit in that link.

5.1.2 Features of MANET

- It is an infrastructure less IP based network of mobile and wireless machine nodes connected with the radio. In operation, the nodes of a MANET does not have centralized administration mechanism.
- It is known for its routeable network properties where each node acts as a "Router" to forward the traffic to other specified node in the network.

Characteristics of MANET:

1. In MANET, each node acts as both host and router. Thus it shows autonomous behavior.
2. Multi-hop radio relaying- When a source node and destination node are out of the radio range, the MANETs are capable of multi-hop routing.
3. It posses distributed nature of operation for security, routing and host configuration. A centralized firewall is absent.
4. The nodes can join or leave the network anytime, making the network topology dynamic in nature.
5. Mobile nodes are characterized by lesser memory, power and lighter in weight features.
6. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
7. It needs mobile and quick behavior which needs minimum human intervention in configuring the network.
8. All nodes possess identical features with similar responsibilities and capabilities and thus it forms a completely symmetric environment.
9. High user density and larger level of user mobility.
10. Nodal connectivity is irregular.

5.1.3 Applications of MANET

- With the increase of portable devices as well as progress in wireless communication Ad-hoc networking is gaining importance with the increasing number of broad applications in the commercial sectors, military and private sectors.
- Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. All nodes in MANETS are mobile and their connections dynamic.
- MANETS do not require a fixed infrastructure. This offers an advantageous decentralized character to the network. The applications of MANET as follows:
  1. **Military Sector**: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of Ad-hoc network came from this field
  2. **Crisis –Management Application**: Ad hoc can be used in emergency rescue operations for disaster management, e.g. in fire, flood, or earthquake. This may be because all of the equipments were destroyed, or perhaps because the region is at remote place. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By

automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier. Other commercial scenarios include e.g. ship-to-ship Ad-hoc mobile communication, law enforcement, etc.

3. **Low Level**: Appropriate low level application might be in domestic networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxi, sports stadium, boat and small aircraft, mobile Ad-hoc communications have many applications.
4. **Data Networks**: A commercial application for MANETS include wide range computing. By allowing computers to forward data to others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.
5. **Vehicular Area Network**: Ad-hoc network is useful in forming network among different vehicles on the road and can propagate information like accidents, congestion. It is also helpful in determining nearby facilities such as gas station, restaurants, hospitals and other facilities.
6. **Personal Area Network**: PAN is short range, localized network where nodes are associated with a given person. These nodes could be attached to someone's cellphone laptop and television and so on.

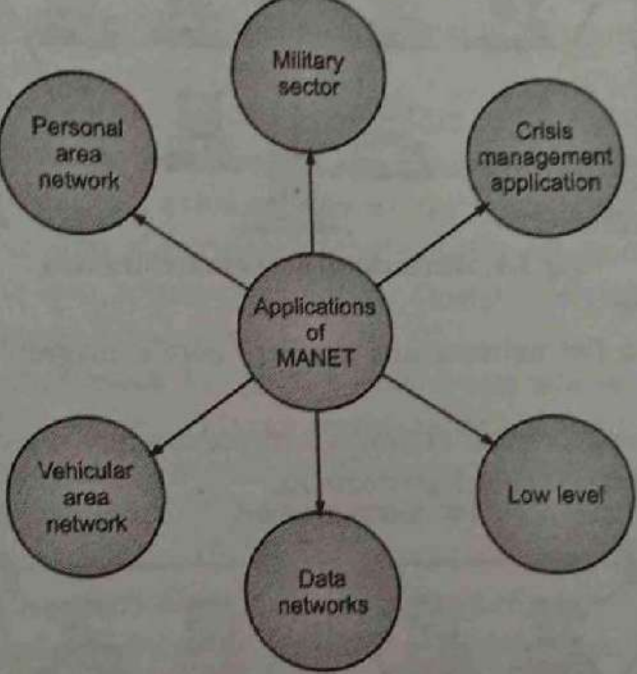


Fig. 5.4 : Applications of MANET

5.1.4 Types of MANET Architecture

- MANET is an autonomous system of mobile host connected by wireless link. In cellular network communication between two Mobile Host (MH) completely rely on the wired backbone and fixed base station.
- There are two approaches to providing network connectivity in a MANET namely, Hierarchical network architecture and Flat-routed architecture.

1. **Hierarchical Network Architecture:**

- A hierarchical network design involves dividing the network into discrete layers. Each layer, or tier, in the hierarchy provides specific functions that define its role within the overall network.

- This helps the network designer and architect to optimize and select the right network hardware, software, and features to perform specific roles for that network layer.
- Hierarchical models apply to both LAN and WAN design. A typical enterprise hierarchical LAN campus network design includes the following three layers:

(i) **Access Layer:** Provides workgroup/user access to the network

(ii) **Distribution Layer:** Provides policy-based connectivity and controls the boundary between the access and core layers

(iii)**Core Layer:** Provides fast transport between distribution switches within the enterprise campus

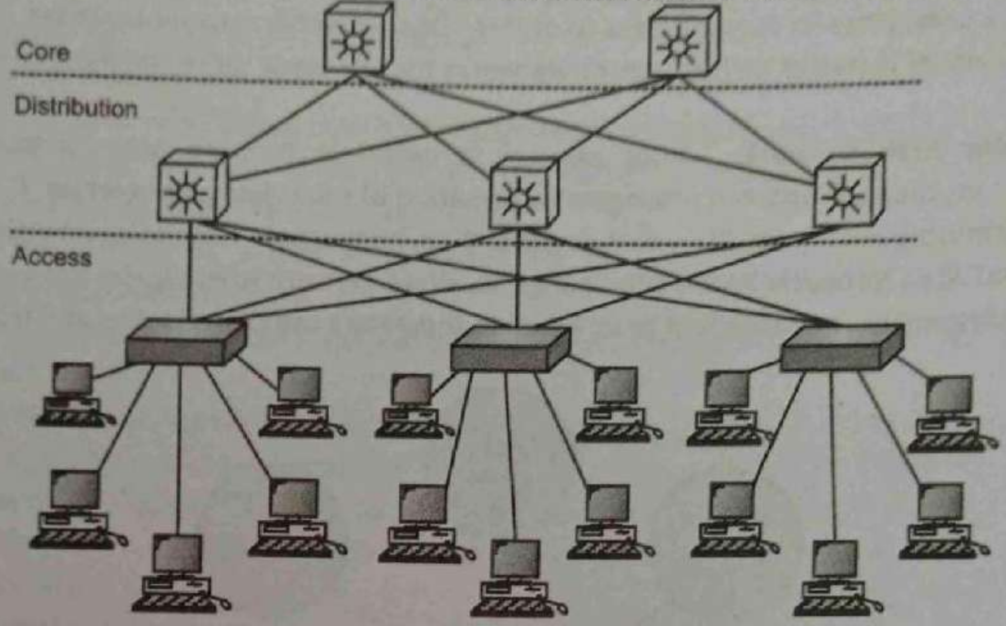


Fig. 5.5 : Hierarchical network architecture

2. **Flat-Routed Architecture:**

- The benefit of dividing a flat network into smaller, more manageable blocks is that local traffic remains local.
- Only traffic that is destined for other networks is moved to a higher layer. The flat network has now been divided into three separate broadcast domains.

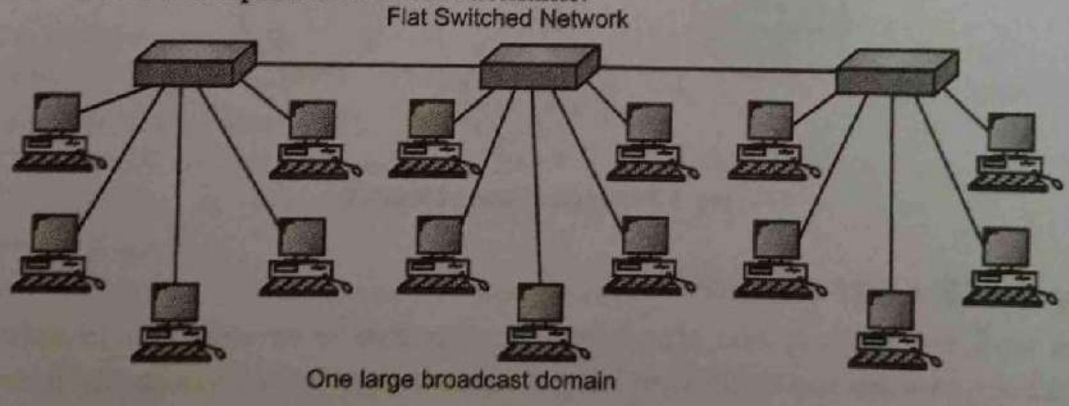


Fig. 5.6: Flat Network

5.1.5 Designing Challenges of MANET

- MANET is defined as a type of Ad-Hoc Network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. It is an autonomous system of mobile host connected by wireless link.

- In cellular network communication between two mobile hosts (MH) completely rely on the wired backbone and fixed base station but in MANET no such infrastructure exists and network topology may dynamically change in an unpredictable manner since nodes are free to move.
- Change in topology made known to other nodes so that outdated topology information can be updated or removed.

Challenges in MANET:

1. **Routing:** Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task, because routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.
2. **Security and Reliability:** An Ad hoc network has its particular security problems due to nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium, mobility-induced packet losses, and data transmission errors.
3. **Quality of Service (QoS):** Providing different quality of service levels in a constantly changing environment will be challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.
4. **Internetworking:** Addition to the communication within an Ad hoc network, inter-networking between MANET and fixed networks is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management
5. **Power Consumption:** For most of the mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.
6. **Restricted Wireless Transmission Range:** The radio group will be restricted in the wireless networks and as a result data amounts it can provide much slighter than what a bound network can provide. This involves routing procedures of wireless networks must be use bandwidth in ideal way. This can be achieved through protecting the overhead as minimum as conceivable. The restricted transmission range also enforces restraint on routing procedures for sustaining the topographical information. Particularly in MANETs because of regular variations in topology, preserving the topological data for every node includes more controller overhead which results in additional bandwidth depletion.
7. **Time-Varying Wireless Link Characteristics:** Wireless channel is liable to a range of broadcast disorders such as path harm, declining, intervention and obstruction. These features resist the series, data rate, and consistency of these cordless transmissions. The range of which these features disturb the transmission that rest on atmospheric situations and flexibility of receiver and transmitter. Even two dissimilar key restraints, Nyquist's and Shannon's theorems that rule over capability to communicate the information at diverse data degrees can be measured.
8. **Packet Losses due to Transmission Errors:** Ad hoc wireless networks practices very advanced packet damage due to reasons such as extraordinary Bit Error Rate (BER) in the wireless channel, enlarged crashes because of the existence of unseen terminals, occurrence of interventions, position reliant controversy, single directional associations, regular pathway breakages due to device movements, and the integral declining characteristics of the wireless passage.

9. **Mobility-Induced Route Changes:** The system topography in ad hoc wireless network is extremely active be-cause of node movement; as a result, a constant meeting undergoes numerous pathway breakages. Such position often results in regular path alterations. So flexibility administration is massive investigation theme in ad hoc networks.
10. **Mobility-Induced Packet Losses:** Communication contacts in an Ad hoc network are insecure such that con-seductively conservative procedures for MANETs over a great damage frequency will suffer from performance deprivation. Though, with large frequency of inaccuracy, it is problematic to supply a data-packet to its target.
11. **Battery Constraints:** It is due to restricted resources that arrange main limitation on the mobile devices in an ad hoc network. Nodes which are contained in such network have restrictions on the supremacy foundation in order to preserve movability, dimension and capacity of the node. Due to accumulation of power and the processing capacity make the nodes heavyweight and less portable. Consequently only MANET devices have to use these resources.

5.1.6 Wireless Sensor Network (WSN)

- A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.
- A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes .The wireless protocol you select depends on your application requirements
- Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.
- Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed.
- WSN is special case of Ad hoc networks with reduced or zero mobility and are known as "Data Centric". That means unlike traditional Ad hoc network where data is requested from specific node or location, here the data is requested based on sensed attributes.
- The use of particular type of query might depend on the application requirements. The query may ask for multiple parameters.
- Sensor node sense the parameters and transmit the values only once or over the period of time or use past history to gain statistical information.

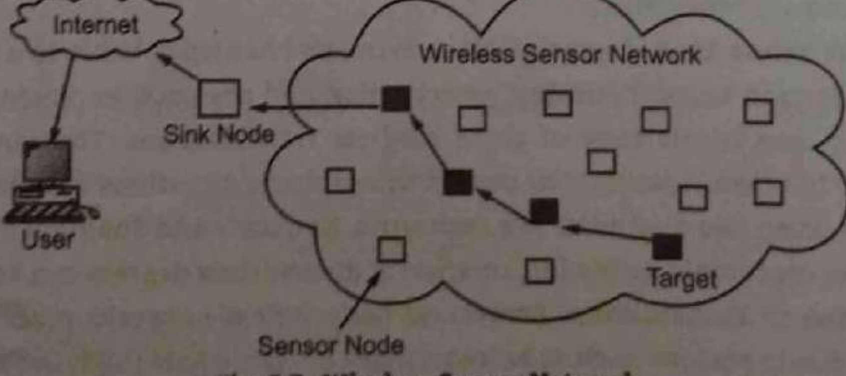


Fig. 5.7 : Wireless Sensor Network

Advantages of WSN:

1. WSN is a flexible network and can adapt to the changes.

2. Additional of New Device: WSN can accommodate new devices in the network any time with ease.
3. Save Cost: Wireless sensor networks save a lot of wiring cost and sensors like PIR detectors are relatively cheaper then wires.

Disadvantages of WSN:

1. WSN networks are not secure as compared to wired networks. Hackers can easily hack the network.
2. Battery Issue: Nodes need to be charged at regular intervals. ...
3. Low Communication Speed: Communication speed is comparatively low than the wired network.

5.2 MESH NETWORKING

- A Wireless Mesh Network (WMN) is a mesh network created through the connection of wireless access points installed. at each network user's locale. Each network user is also a provider, forwarding data to the next node.
- The networking infrastructure is decentralized and simplified because each node need only transmit as far as the next node.
- Wireless mesh networking could allow people living in remote areas and small businesses operating in rural neighborhoods to connect their networks together for affordable Internet connections.
- Wireless Mesh Network (WMN) has recently being emerged as trend for the next generation wireless network.

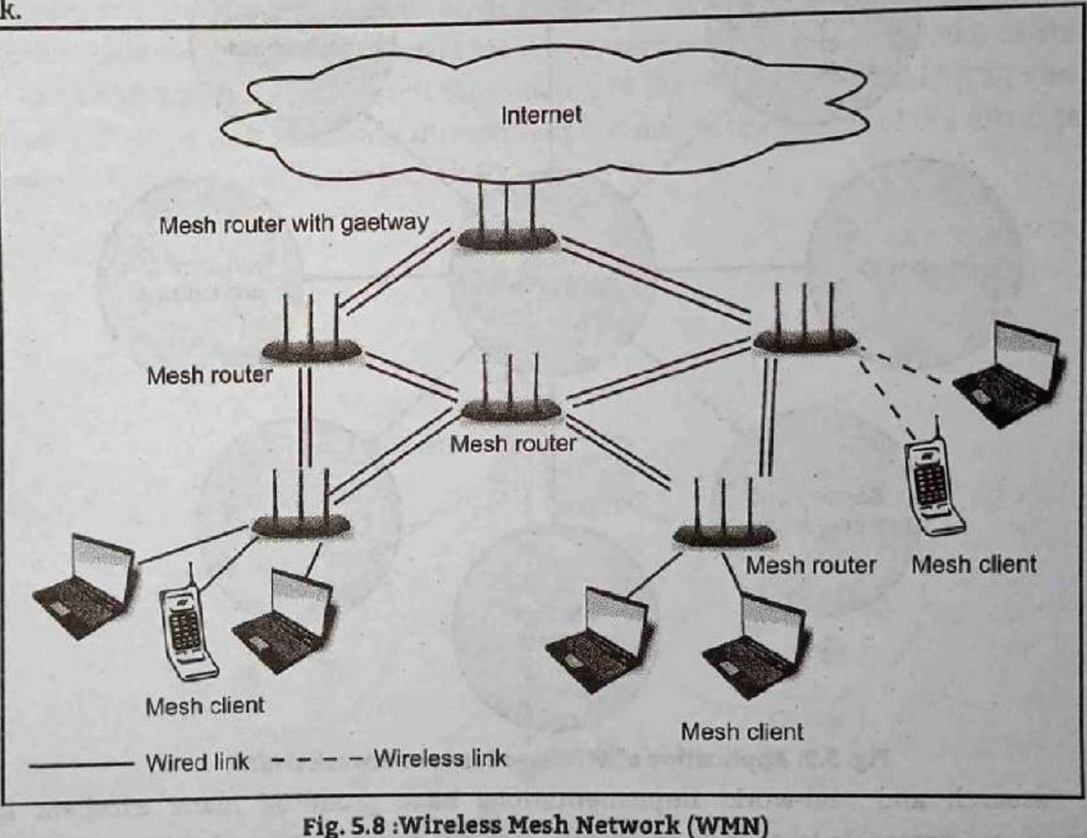


Fig. 5.8 :Wireless Mesh Network (WMN)

- Wireless Mesh Network (WMN) combines multi hop and multi cell fashion with no mobility of cells.
- Wireless Mesh Network (WMN) employs AP known as IGW (Internet gateway) to provide network access service for Mobile Host (MH).
- To have larger coverage, WMN employs a relay station known as "Mesh Router "in Ad-hoc mode. Ad hoc network technology enables the MR to establish a mesh like network with no mobility to MR.

- This mesh router enables relay of packets originated at MH by wireless radio links.
- WMN uses a key technology –Self organization, it constructs the network without centralized control.

5.2.1 Applications of WSN

- Wireless Sensor Networks (WSN) is an important and exciting new technology with great potential for improving many current applications in medicine, transportation, agriculture, industrial process control, and the military as well as creating new revolutionary systems in areas such as global-scale environmental monitoring, precision agriculture,
- home and assisted living medical care, smart buildings and cities, and numerous future military applications. In fact, it is difficult to consider any major application area that cannot benefit from WSN technology.
- Typically, WSN are composed of large numbers of minimal capacity sensing, computing, and communicating devices and various types of actuators. WSN operate in complex and noisy real world, real-time environments.

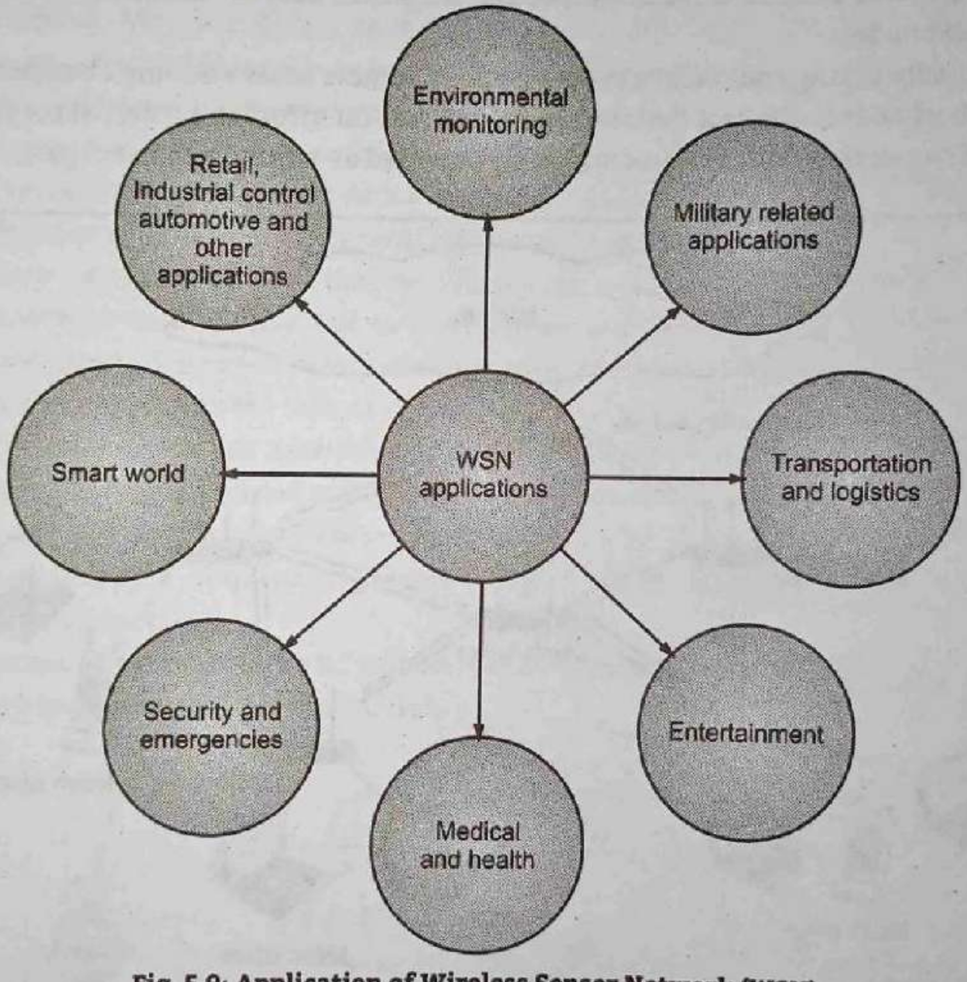

Environmental monitoring
Retail, Industrial control automotive and other applications
Military related applications
Smart world
WSN applications
Transportation and logistics
Security and emergencies
Entertainment
Medical and health

Fig. 5.9: Application of Wireless Sensor Network (WSN)

- To date, research and real-world implementations have produced many excellent low level mechanisms and protocols to collect, transport, perform sensor fusion of this raw data and react with control actions.

1. **Surveillance Applications:** VigilNet is a military wireless sensor network that acquires and verifies information about enemy capabilities and positions of hostile targets. It has been successfully designed, built, demonstrated, and delivered to the Defense Intelligence Agency for

realistic deployment. To accomplish different mission objectives, the VigilNet system consists of 40,000 lines of code, supporting multiple existing mote platforms including MICA2DOT, MICA2, and XSM.

2. **Body Area Network:** Specialized sensors and transducers are developed to measure human body characterizing parameters so that human conditions could be predicted efficiently and accurately

3. **Environmental Monitoring:** Use of sensors in monitoring the landfill and the air quality. Deployment of large number of sensors allows real time monitoring of gases being emitted by waste material or from hazardous air pollutants

4. **Drinking Water Quality:** The main objective is to develop data mining technique to water quality databases and use them for interpreting using environmental data which helps in addition of chlorine to the treated water before releasing to the distribution system.

2.2 Clustering of WSN

Clustering is partitioning of sensor network which not only allows aggregation of sensed data but limits data transmission primarily within the cluster that reduces both traffic as well as contention for channel clustering.

Beacon signals are transmitted for determining the close by Sensor Nodes. Nearby Sensor Nodes with some intermediate Sensor Nodes forming clusters.

Sensor nodes in a cluster can transmit directly to their respective Cluster Head (CH) without any intermediate sensor nodes .This minimizes the energy consumed within individual clusters.

Cluster Head (CH) also need to transmit information to the other Cluster Head (CH) and the energy consumed in wireless transmission is directly proportional to the square of the distance d between the sensor nodes acting as a Cluster Head (CH).

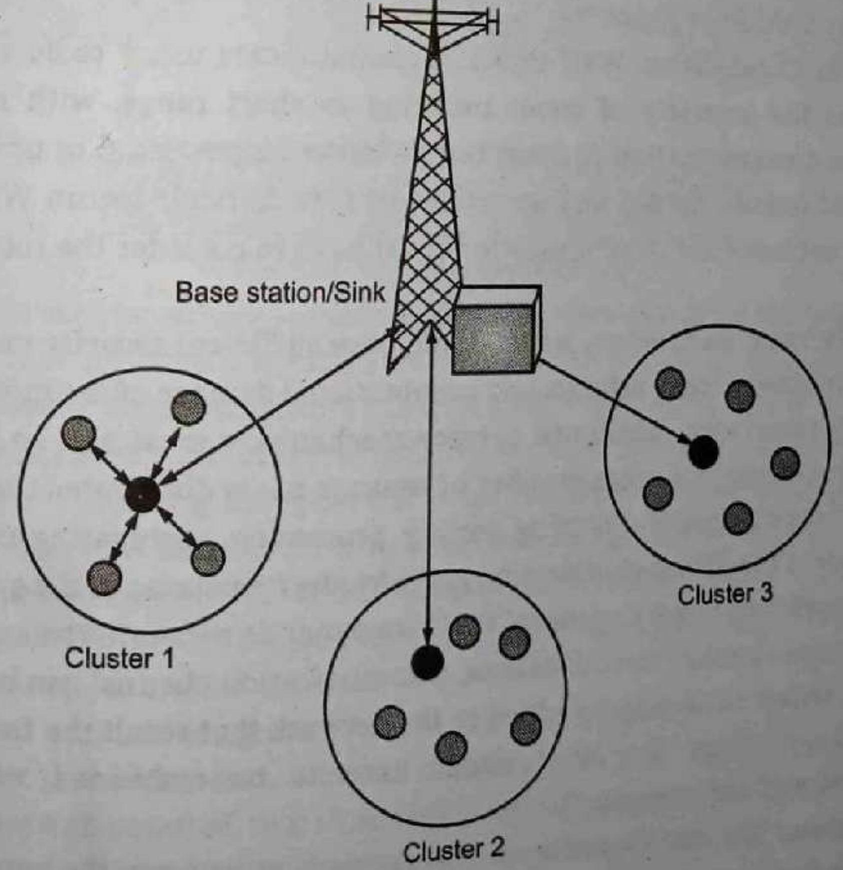


Fig. 5.10: Clustering of Sensor Node

- Therefore it is desirable to partition a Wireless Sensor Network (WSN) into cluster in such a way that all the sensor nodes in a cluster reachable by path length less than distance d to Cluster Head (CH).
- Determining optimal value of distance d that minimizes overall energy consumption, is very complex problem and it also need to take into account of data to be transferred within each cluster and between clusters, frequency of transmission, maximum allowable latency.
- To select Cluster Head (CH) usually the sensor node with highest degree (Largest number of neighbors) is selected. As Cluster Head (CH) does aggregation of data received from its cluster members, it is usually trusted with transmission schedule to its members and the Base station (BS).
- Cluster Head (CH) needs to perform more functions than sensor nodes it may run out of energy at a much faster rate. Hence dynamically changing Cluster Head (CH) has been suggested so as to distribute energy consumption as evenly as possible.

5.2.3 Characteristics of WSN

- WSN is currently used for real-world unattended physical environment to measure numerous parameters. So, the characteristics of WSN must be considered for efficient deployment of the network.
- The significant **characteristics of WSN** are described as follows:
  1. **Low Cost**: In the WSN normally hundreds or thousands of sensor nodes are deployed to measure any physical environment. In order to reduce the overall cost of the whole network the cost of the sensor node must be kept as low as possible.
  2. **Energy Efficient**: Energy in WSN is used for different purpose such as computation, communication and storage. Sensor node consumes more energy compare to any other for communication. If they run out of the power they often become invalid as we do not have any option to recharge. So, the protocols and algorithm development should consider the power consumption in the design phase.
  3. **Communication Capabilities:** WSN typically communicate using radio waves over a wireless channel. It has the property of communicating in short range, with narrow and dynamic bandwidth. The communication channel can be either bidirectional or unidirectional. With the unattended and hostile operational environment it is difficult to run WSN smoothly. So, the hardware and software for communication must have to consider the robustness, security and resiliency.
  4. **Security and Privacy**: Each sensor node should have sufficient security mechanisms in order to prevent unauthorized access, attacks, and unintentional damage of the information inside of the sensor node. Furthermore, additional privacy mechanisms must also be included. Distributed sensing and processing: the large number of sensor node is distributed uniformly or randomly. WSNs each node is capable of collecting, sorting, processing, aggregating and sending the data to the sink. Therefore the distributed sensing provides the robustness of the system.
  5. **Dynamic Network Topology**: In general WSN are dynamic network. The sensor node can fail for battery exhaustion or other circumstances, communication channel can be disrupted as well as the additional sensor node may be added to the network that result the frequent changes in the network topology. Thus, the WSN nodes have to be embedded with the function of reconfiguration, self-adjustment.
  6. **Self-Organization**: The sensor nodes in the network must have the capability of organizing themselves. As the sensor nodes are deployed in an unknown fashion in an unattended and

hostile environment. The sensor nodes have work in collaboration to adjust themselves to the distributed algorithm and form the network automatically.

7. **Multi-Hop Communication**: Large numbers of sensor nodes are deployed in WSN. So, the feasible way to communicate with the sinker or base station is to take the help of an intermediate node through routing path. If one needs to communicate with the other node or base station which is beyond its radio frequency it must me through the multi-hop route by intermediate node.
8. **Application Oriented**: WSN is different from the conventional network due to its nature. It is highly dependent on the application ranges from military, environmental as well as health sector. The nodes are deployed randomly and spanned depending on the type of use.
9. **Robust Operations**: Since the sensors are going to be deployed over a large and sometimes hostile environment. So, the sensor nodes have to be fault and error tolerant. Therefore, sensor nodes need the ability to self-test, self-calibrate, and self-repair Small physical size: sensor nodes are generally small in size with the restricted range. Due to its size its energy is limited which makes the communication capability low.

5.2.4 Block Diagram of Sensor Node

- A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.
- A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes.
- The block diagram of sensor node is shown in Fig. 5.11.

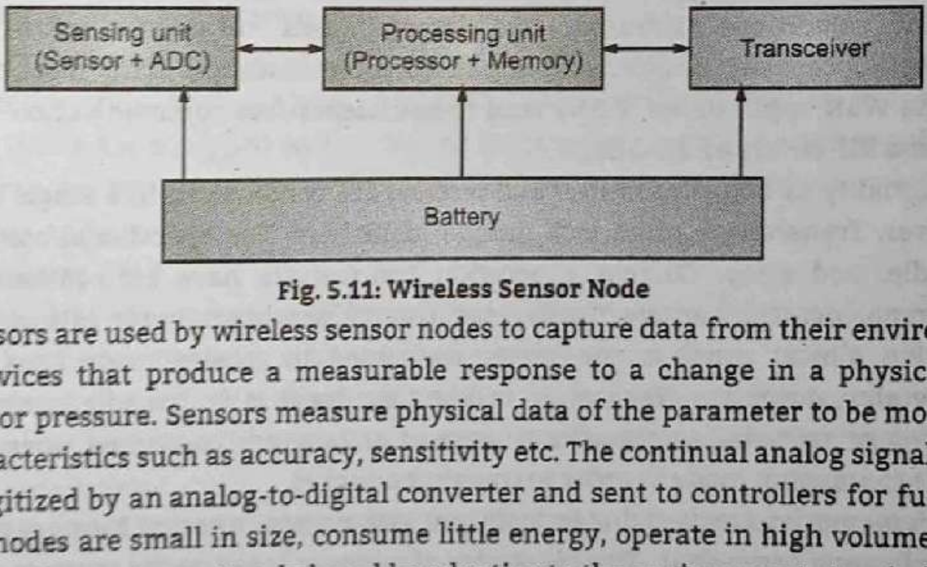


Fig. 5.11: Wireless Sensor Node

- **Sensors**: Sensors are used by wireless sensor nodes to capture data from their environment. They are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored and have specific characteristics such as accuracy, sensitivity etc. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing. Most sensor nodes are small in size, consume little energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

  Sensors are classified into two categories: Passive and Active sensors.

  1. **Passive sensors** sense the data without actually manipulating the environment by active probing. They are self-powered; that is, energy is needed only to amplify their analog signal.
  2. **Active sensors** actively probe the environment, for example, a sonar or radar sensor, and they require continuous energy from a power source.

Most theoretical work on WSNs assumes the use of passive sensors. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing. Several sources of power consumption in sensors are: signal sampling and conversion of physical signals to electrical ones, signal conditioning, and analog-to-digital conversion. Spatial density of sensor nodes in the field may be as high as 20 nodes per cubic meter.

- **Microcontroller**: The controller performs tasks, processes data and controls the functionality of other components in the sensor node. While the most common controller is a microcontroller, other alternatives that can be used as a controller are: a general purpose desktop microprocessor, digital signal processors, FPGAs (Field Programmable Gate Array) and ASICs (Application Specific Integrated Circuits).
  - A microcontroller is often used in many embedded systems such as sensor nodes because of its low cost, flexibility to connect to other devices, ease of programming, and low power consumption. A general purpose microprocessor generally has higher power consumption than a microcontroller; therefore it is often not considered a suitable choice for a sensor node.
  - Digital Signal Processors may be chosen for broadband wireless communication applications, but in Wireless Sensor Networks the wireless communication is often modest: i.e., simpler, easier to process modulation and the signal processing tasks of actual sensing of data is less complicated. Therefore, the advantages of DSPs are not usually of much importance to wireless sensor nodes. FPGAs can be reprogrammed and reconfigured according to requirements, but this takes more time and energy than desired.
- **Transceivers**: Sensor nodes often make use of ISM band, which gives free radio, spectrum allocation and global availability. The possible choices of wireless transmission media are radio frequency (RF), optical communication (laser) and infrared.
  - Lasers require less energy, but need line-of-sight for communication and are sensitive to atmospheric conditions. Infrared, like lasers, needs no antenna but it is limited in its broadcasting capacity. Radio frequency-based communication is the most relevant that fits most of the WSN applications. WSNs tend to use license-free communication frequencies: 173, 433, 868, and 915 MHz; and 2.4 GHz.
  - The functionality of both transmitter and receiver are combined into a single device known as a transceiver. Transceivers often lack unique identifiers. The operational states are transmit, receive, idle, and sleep. Current generation transceivers have built-in state machines that perform some operations automatically. Most transceivers operating in idle mode have a power consumption almost equal to the power consumed in receive mode. Thus, it is better to completely shut down the transceiver rather than leave it in the idle mode when it is not transmitting or receiving. A significant amount of power is consumed when switching from sleep mode to transmit mode in order to transmit a packet.
- **Memory**: Flash memories are used due to their cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage are:
  1. User memory used for storing application related or personal data and
  2. Program memory used for programming the device. Program memory also contains identification data of the device.

5.2.5 Different Types WSN Architecture

- Depending on the environment, the types of networks are decided. Hence different types of WSNs include Terrestrial WSNs, Underground WSNs, Underwater WSNs, Multimedia WSNs and Mobile WSNs.

1. **Terrestrial WSNs:**

- Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured (Ad hoc) or structured (Preplanned) manner.
- In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane.
- The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models. In this WSN, the battery power is limited; however, the battery is equipped with solar cells as a secondary power source.
- The Energy conservation of these WSNs is achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

2. **Underground WSNs:**

- The underground wireless sensor networks are more expensive than the terrestrial WSNs in terms of deployment, maintenance, and equipment cost considerations and careful planning.
- The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.
- The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power are difficult to recharge.
- In addition to this, the underground environment makes wireless communication a challenge due to high level of attenuation and signal loss.

3. **Under Water WSNs:**

- More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water.
- Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures.
- Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

4. **Multimedia WSNs:**

- Multimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio.
- These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are interconnected with each other over a wireless connection for data compression, data retrieval and correlation.
- The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

5. **Mobile WSNs:**

- These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate.
- The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency, superior channel capacity, and so on.

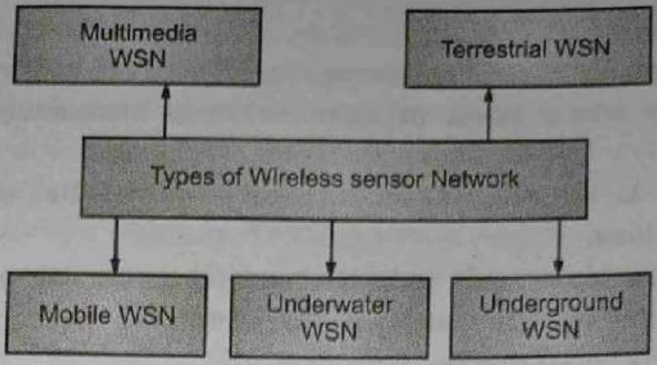


Fig. 5.12: Types of WSN architecture

5.2.6 Energy Efficiency in WSN

- Fig. 5.13 shows classification of energy efficiency mechanism in WSN.

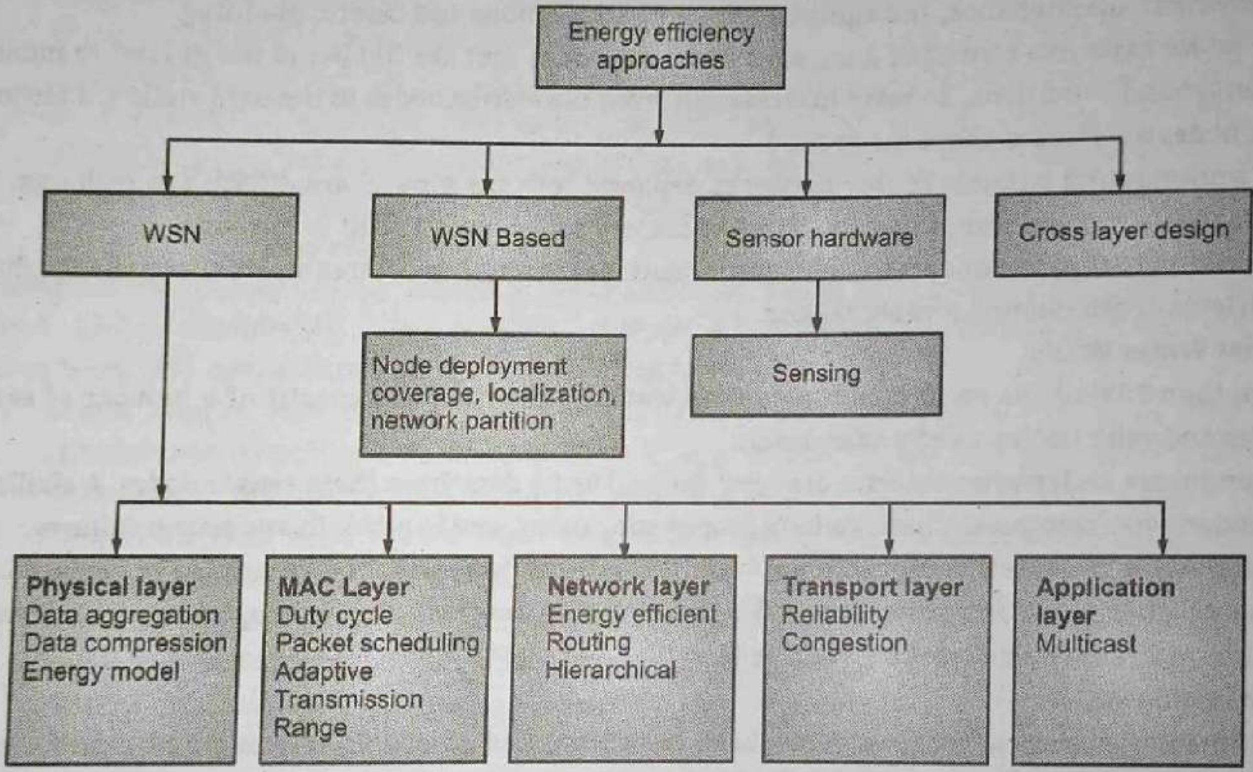


Fig. 5.13 : Classification of energy efficiency mechanism in WSN

- The classification of Energy efficiency mechanisms in WSNs can be classified as WSN Protocol Stack, WSN based Techniques, Sensor Hardware and Cross layer design.
- **WSN Protocol Stack:** The energy efficient techniques under WSN Protocol Stack can be further classified as physical layer, mac layer, network layer, transport layer and application layer.
  1. **Physical Layer:** Modulation, transmission and receiving techniques are importance of physical layer. In multi hop Wireless Sensor Network (WSN): Distance, Transmission energy, Modulation Scheme. Energy efficiency can be increased by proper Modulation scheme.
  2. **MAC Layer:** The MAC layer has to be responsible for reliability, energy efficiency, high throughput and low access delay to optimally utilize the energy-limited resources of sensor nodes. Maximum amount of energy wasted in MAC protocol operations like collision, overhearing, control packet overhead and interference. To minimize the energy expenditure at WSNs energy efficient MAC techniques like duty cycling, packet scheduling adaptive

transmission range, and adaptive transmission period. A duty cycling in MAC layer involves the sensor node to sleep/wake up mechanisms to conserve energy. Sleep/wake up mechanisms involves in putting the radio transceiver in the (low-power) sleep mode whenever communication is not required. Ideally, the radio should be switched off as soon as there is no more data to send/receive, and should be resumed as soon as a new data packet becomes ready. The mechanism which makes the sensor nodes to alternate between active and sleep periods depending on network activity can be referred as duty cycling.

3. **Network Layer:** Routing is the process which finds the path between the source to destination while initiating data communication in the network. Routing is much more important than any other networks compared to WSNs.

Table 5.1 : Radio characteristics

Radio Mode	Energy Consumption
Transmitter Electronics (ElecTx) Receiver Electronics (E–elecRx) (Eelec = EelecRx = EelectTx)	50nJ/bit
Transmit Amplifier (εamp)	100 pJ/bit/m^2
Idle (Eidle)	40nJ/bit
Sleep	

The energy spent in communication (transmission and reception) is much higher than Idle and sleep state of the sensor node. Energy efficient routing can be done through Cluster based hierarchical Routing, flat routing, multipath routing, and geographical routing.

LEACH Protocol is a kind of cluster-based routing protocols, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. In LEACH, the CH nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the BS in order to reduce the amount of information that must be transmitted to the BS. LEACH uses a Time division multiple access (TDMA) and code-division multiple access (CDMA) MAC to reduce inter-cluster and intra-cluster collisions. Cluster heads change randomly over time in order to balance the energy dissipation of nodes

4. **Transport Layer:** When multiple nodes want to transmit data through the same channel at a time or when the routing node fails to forward the received data to the next routing nodes congestion occurs. Congestion and data loss occurs at nodes which are nearer to the sink nodes. Energy saving can be achieved in transport layer of WSNs through energy aware congestion avoidance, energy efficient load sharing and energy efficient reliable mechanisms between end to end communication in WSNs.

5. **Application layer:** Energy saving in the application layer is achieved through application service which aims at energy conservation, by caching mutable data obtained from data-retrieval at locations that minimize the sum of request and update traffic & asynchronously multicasting updates from sensors to observers reduces the total number of packet transmissions in the network.

WSN Based Techniques

- Energy Efficient Deployment in WSN : The optimal deployment of nodes adds to the lifetime of the network, along with determination of deployment cost, coverage, connectivity, etc. A good deployment is important to achieve load balance and prolong the network lifetime

- **Energy Efficient Coverage in WSNs:** The main objective of the area coverage in WSNs is to cover a region (the collection of all space points within the sensor field), and each point of the region need to be monitored. Point coverage is to cover a set of point (target) with known location that need to be monitored. The point coverage scheme focuses on determining sensor nodes' exact positions, which guarantee efficient coverage application for a limited number of immobile points (targets). The coverage issues improve minimization of power utilization of WSNs and WSNs lifetime

- **Sensor Hardware**

  The energy consumption in WSN hardware involves three different components

  1. Sensing Unit (Sensing Transducer and ADC)
  2. Communication Unit (Transmitter and receiver radio)
  3. Computing and Processing Unit
     - **Sensing Transducer:** The energy consumption of this part depends on the Hardware and Application. Sensing energy is the small fraction of the total energy consumed.
     - **ADC:** ADC for sensor consumes only 3.1µW,in 31pJ/8 bit-sample at 1volt supply. The standby power consumption at 1V supply is 41pW.
     - **Transmission Energy:** Transmission energy transmits a k-bit message to distance d can be computed as :

       $$E_{TX}(k,d) = E_{\cdot elec\cdot}(k)+\epsilon.\ k.d^2$$

       k = no. of bits per messages

       d = distance between the SN

       $E_{\cdot elec}$ = Transmission electronic energy consumption.

     - **Receiver Energy:** To receive k bit message the energy consumed is

       $$E_{RX}(k) = E_{\cdot elec\cdot}(k)$$

     - **Computation :** The computing unit associated with a WS is a microcontroller /Processor with memory which can control and operate the sensing ,computing and communication unit. The energy consumption of this unit has mainly two parts: Switching Energy, Leakage Energy .

       Switching Energy is given by

       $$\text{Switching energy} = \text{Eswitch}=\text{Ctotal}*\text{Vdd}^2$$

       Where ,

       Vdd = supply voltage.

       Ctotal = Total capacitance switched by computation.

     - **Leakage Energy:** This is the energy consumed when no computation work is done.

       The energy consumed in one bit of data can be used to perform large number of arithmetic operations in the sensor processor.

     - **Residual Energy:** the remaining energy of sensor node is known as residual energy which reflects how long the sensor node can perform all its functions correctly.

5.2.7 Designing Challenges in WSN

- Wireless Sensor Network (WSN) is special case of ad-hoc networks with reduced or no mobility and are known as "Data Centric". This means, unlike traditional ad hoc network where data is requested from specific node or location, data is requested based on sensed attributes.
- The use of particular type of query might depend on the application requirements. The major factors that need to considered while designing sensor network are listed below:

1. **Scalable and Flexible Architecture:** In the sensor network the number of sensor nodes deployed may be order of hundred, thousands or millions so that we can easily extend the network size. The communication protocols must be designed in such a manner that deploying many nodes in the network does not affect clustering and routing. In other words, the network must preserve its stability. Introducing more nodes into the network means that additional communication messages will be exchanged, so that these nodes are integrated into the existing network.
2. **Error-Prone Wireless Medium:** Since sensor networks can be deployed in different situations, the requirements of each different application may vary significantly. We should consider that the wireless medium can be greatly affected by noisy environments. An attacker interferes knowingly and causes enough noise to affect the communication.
3. **Fault Tolerance and Adaptability:** Fault tolerance means to maintain sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't affect the overall task of the sensor network. Adaptable protocols can establish new links in case of node failure or link congestion. Network can able to adapt by changing its connectivity in case of any fault. In that case, well- efficient routing algorithm is applied to change the overall configuration of network.
4. **Infrastructure:** Sensors network are infrastructure less in which nodes can communicate directly with base station. It utilizes multi-hop radio relaying and number of base station depends upon area covered by node and its radio range.
5. **Node Deployment:** Sensor network can be deployed randomly in geographical area. After deployment, they can be maintained automatically without human presence. In sensor network node deployment falls into two categories either a dense deployment or a sparse deployment. In dense deployment we have relatively high number of sensor nodes in the targeted field while in a sparse deployment we have fewer nodes and it is used when the cost of sensor nodes increases and prohibited the use of dense deployment. The dense deployment is used when it is important to detect the every moment or when we have multiple sensors for covering an area.
6. **Real Time:** Achieving Real-time in WSN is difficult to maintain. It must support maximum bandwidth, minimum delay and several QOS parameters. This issue can affect time synchronization algorithm.
7. **Dynamic Changes:** As in sensor network nodes are deployed without any topology and they are adaptable to changes due to addition of new nodes or failure of nodes. Thus, unlike traditional networks, where the goal is to maximize the channel throughput or minimize the node deployment, but in a sensor network focus is to extend the system lifetime and the system robustness.
8. **Power Consumption** : Wireless sensor node is microelectronic device means it is equipped with a limited number of power source. Nodes are dependent on battery for their power. Hence power conservation and power management is an important issue in wireless sensor network. Due to this reason researchers are focusing on the design of power aware protocols and algorithm for sensors network.
9. **Production Cost:** As the name suggests production cost, we know that in the sensor network we have large no of nodes deployed, so if a single node will be very high then the cost of over all network will be very high. As a result the cost of each sensor node has to be kept low. In order to make sensor network feasible the cost of sensor node should be less. As a result the cost of sensor node will be a very challenging issue.

10. **Short Range Transmission:** In WSNs we should consider the short transmission range in order to reduce the possibility of being eavesdropped. As in long range transmission we need high transmission power due to the point to point transmission between the nodes to reach the destination which increases the chance of being eavesdropped.
11. **Hardware Design:** While designing any hardware of sensor network, it should be energy-efficient. Hardware such as micro-controller, power control, and communication unit should be design to consume less energy.
12. **Limited Computational Power and Memory Size:** It is another factor that affects WSN in the sense that each node stores the data individually and sometime more than one node stored same data and transferred to the base station which waste the power and storing capacity of nodes so we must develop effective routing schemes and protocols to minimize the redundancy in the network.
13. **Operating Environment:** Sensor nodes are deployed densely either very closed or inside the phenomenon which is to be observed. These nodes may work under-busy interaction, at the bottom of an ocean, in the interior of a large machinery, on the surface of an ocean during a tornado, in a home or large building and in a large warehouses.
14. **Simplicity:** Simplicity is an important point in the wireless sensor network since sensor nodes are small and there is restriction on the utilization of energy as they are energy dependent so the computing and communicating software used in the nodes should be computation efficient and less in size than the traditional software in the network
15. **Quality of Service:** It means data should be delivered within time period. Some real time sensor applications are based on time means if data should not be delivered on time from the moment it is sensed; the data will become unusable for e.g. fire detection requires good quality of services.
16. **Security:** Security is very important parameter in sensor network since sensor networks are data centric so there is no particular id associated with sensor nodes and attacker can easily inserted himself into the network and stole the important data by becoming the part of network without the knowledge of sensor nodes of the network. So it is difficult to identify whether the information is authenticated or not.

5.2.8 Internet of Things (IoT)

- Nowadays many companies are jumping for "Internet of Things". Even Indian Government came up with policy paper in their Ministry of Information Technology. By looking towards words, there are two words, one is "Internet" and other word is "Things".
- In simple way we can say "Internet of things" is to do operations(things) smartly using Internet. What are these operations, these operations can be any intelligent work which will induce smartness in the devices.
- For example our home made "electric meters", now company person is coming at every bodies home to read your power consumption.
- If Electric meter started sending your electric consumption to directly to computer server (cloud server), we have saved so many man hours which we can use for other work or reduce work force so that electric companies can become more competitive.
- The definition of a "Thing" in the Internet of Things varies a lot. "Thing" as an embedded computing device (or embedded system) that transmits and receives information over a network for the purpose of controlling another device or interacting with a user.

- "Things" of IoT are sensing or actuating, processing, or communicating. Things can be small device which can survive by own for many years.
- We should able to put this device in to Dam bridges or soil which will work for years and keep sending signals to the Gateway. This Gateway can support various technologies for communication.
- It is not necessary that Devices should send signals by wire signal, Device can use wireless, pinging, variety of ways. There should be more scope in the protocols to accommodate theses communicating technologies. Other best part of IoT is Local Networks.

Comparison between MANET, WSN and IoT:

Table 5.2

Sr. No	Feature	Wireless Sensor Network	Ad hoc Network	IOT
1.	Number of sensor nodes or motes	Large in quantity	Medium in quantity	Less in quantity
2.	Deployment type	Very much dense	Scattered	Scattered
3.	Rate of failure	Prone to failures	Very rare	Less
4.	Change in network topology	Dynamically	*Dynamically	Less
5.	Communication mode	Peer to Peer	Peer to peer and end to end	• Point to Point (P2P) • Star • Mesh • Hybrid [24]
6.	Battery	Not replaceable /not rechargeable	Replaceable	Replaceable
7.	Identifiers (IDs) used in the network	No unique IDs	Unique IDs	Unique IDs
8.	Centric mode	Data centric	Address centric	Both
9.	Fusion/Aggregation	Possible	Not suitable	Possible
10.	Computational capacities and memory requirement	Limited	Not limited	Limited
11.	Data rate support provided	Lower	Higher	Moderate
12.	Redundancy	High	Low	Low
13.	Standards	ZigBee, IEEE 802.15.4, ISA100, IEEE 1451	IEEE 802.11	ZigBee, RFID, Bluetooth and BACnet
14.	Fault tolerance	Needed only if nodes exhaust available energy or are moved	Needed as mobility increases	Absence of access to the running code, Denial-of-service for heterogeneous hardware [30]
15.	Communication Range	Short	Long	Long
16.	Interaction	Focus on interaction with the environment	Close to humans e.g. laptops, PDAs, mobile radio terminals	Machine-to Machine Interaction

Table 5.3 : Comparison of WSN and MANET

Sr. No.	Parameters	Wireless Sensor Networks	Ad Hoc Networks
1.	Number of sensor nodes	Large	Medium
2.	Deployment	Densely deployed	Scattered
3.	Failure rate	Prone to failures	Very rare
4.	Topology	Dynamic	Dynamic
5.	Communication paradigm	Peer to Peer	Peer to peer and end to end
6.	Battery	Not replaceable /not rechargeable	Replaceable
7.	Identifiers	No unique identifiers	Unique identifiers
8.	Centric	Data centric	Address centric
9.	Fusion / aggregation	Possible	Not suitable
10.	Computational capacities and memory	Limited	Not limited
11.	Data rate	Low	High
12.	Redundancy	High	Low
13.	Routing protocols	Flooding, Gossiping, Flat Routing, Hierarchical, Location based	Pro-active, Reactive, Hybrid
14.	Standards	ZigBee, IEEE 802.15.4, ISA100, IEEE 1451	IEEE 802.11
15.	Fault tolerance	Needed only if nodes exhaust available energy or are moved	Needed as mobility increases
16.	Communication Range	Short	Long

5.3 ISO EQUIVALENT PROTOCOL LAYER ARCHITECTURE FOR WSN

- Fig. 5.14 shows WSN protocol architecture.
- The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers.
- Mostly in sensor network require five layers, namely application, transport, network, data link and physical layer. The three cross planes are namely power management, mobility management, and task management.
- These layers of the WSN are used to accomplish the network and make the sensors work together in order to raise the complete efficiency of the network.

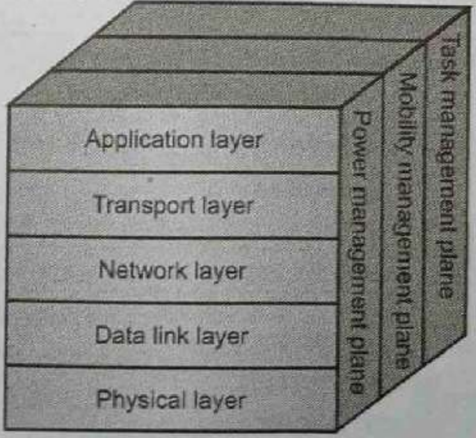


Fig. 5.14: WSN Protocol Architecture

Physical Layer:

- The physical layer provides an edge for transferring a stream of bits above physical medium. This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation and data encryption.
- IEEE 802.15.4 is suggested as typical for low rate particular areas and wireless sensor network with low cost, power consumption, density, the range of communication to improve the battery life.

Data Link Layer:

- The data link layer is responsible for multiplexing of data streams, frame detection, Media Access Control (MAC) and error control.
- Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbors' broadcast.

Transport Layer:

- The function of the transport layer is to deliver congestion avoidance and reliability where a lot of protocols intended to offer this function are either practical on the upstream.
- These protocols use dissimilar mechanisms for loss recognition and loss recovery. The transport layer is exactly needed when a system is planned to contact other networks.
- Providing a reliable loss recovery is more energy efficient and that is one of the main reasons why TCP is not fit for WSN. In general, Transport layers can be separated into Packet driven, Event driven.

Network Layer:

- The main function of the network layer is routing, it has a lot of tasks based on the application, but actually, the main tasks are in the power conserving, partial memory, buffers, and sensor don't have a universal ID and have to be self-organized.
- The simple idea of the routing protocol is to explain a reliable lane and redundant lanes, according to a convinced scale called metric, which varies from protocol to protocol.
- There are a lot of existing protocols for this network layer, they can be separate into; flat routing and hierarchal routing or can be separated into time driven, query-driven & event driven.
- There are some popular protocols in the transport layer namely STCP (Sensor Transmission Control Protocol), PORT (Price-Oriented Reliable Transport Protocol and PSFQ (pump slow fetch quick).

Application Layer:

- The application layer is liable for traffic management and offers software for numerous applications that convert the data in a clear form to find positive information.
- Sensor networks arranged in numerous applications in different fields such as agricultural, military, environment, medical, etc.

Power, Mobility and Task Management Planes:

- In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes.
  1. **Power Management Planes:** It manages how a sensor node uses its power. When the power level of a sensor node is low, the sensor node broadcast to its neighbors that it is low in power and cannot participate in routing message. The remaining power is reserved for sensing.
  2. **Mobility Management Planes:** It detect and register the movement of sensor nodes; so a route back to the user is always maintained. The sensor nodes can keep track of who their neighbor sensor node are and then sensor nodes can balance their power task usage.
  3. **Task Management Plane:** It balances and schedules the sensing task given to specific region. These planes help the sensor nodes coordinate the sensing task and lower the overall energy consumption.

5.3.1 Classification of Clustering Algorithms

- There have been several different methods to classify the algorithms used for WSNs Clustering. Four of the most common classifications are shown in Fig. 5.15.

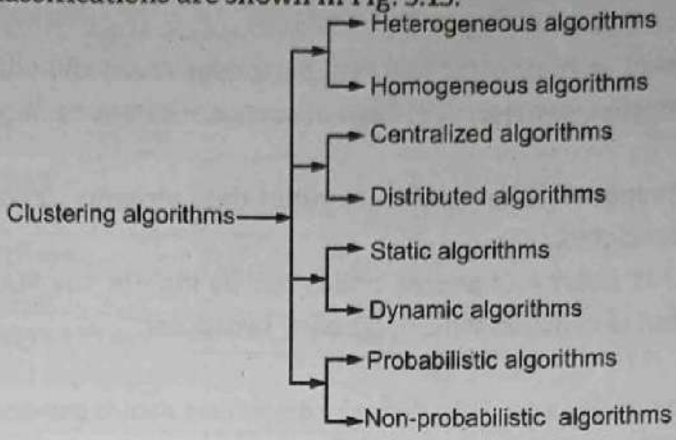


Fig. 5.15 : Common Classification Algorithm

- **Clustering Algorithms Homogeneous or Heterogeneous Networks:** This classification according to the characteristics and performance of sensor nodes in a cluster. In heterogeneous sensor networks, all nodes have the same specifications, hardware and processing capabilities. In these networks, which are common in nowadays applications, each node can be a CH. In addition to these networks, the CH role can be replaced between the nodes periodically (for the creation of better and more integrated load balancing energy). Against in heterogeneous sensor networks, generally, there are two types of sensor, the first type sensors with more processing abilities and complex hardware. These sensors predetermined as a CH node. The other type conventional sensors, with lower abilities, which in fact, used to sense the environment properties.
- **Centralized or Distributed Clustering Algorithms:** These clustering algorithms imply on the method utilized for shaping clusters. A distributed CH selection and shaping process are the most suitable way to obtain enhanced flexibility and faster convergence times independent of the number of nodes of the WSN. This approach is the most efficient method, particularly for large networks. Also, there are a few approaches using centralized or hybrid method, which one or more coordinate nodes or base stations (sink), responsible for the break up into detached and control of all network cluster members. These networks are not appropriate for overall objective large-scale practical application WSNs. They may be appropriate just for specific targets bounded-scale applications in which high-quality connectivity and network separation is needed.
- **Static and Dynamic Clustering Algorithms:** Other conventional classification is static or dynamic clustering. Process shaping clusters is dynamic (otherwise as static) when it contains regular (periodic or event-oriented) CH re-election or includes cluster reorganization routine, these procedures may be effective in order to respond to changes in network topology and only accurately the cluster topology or proper movement with the purpose CH role between the nodes to obtain in energy saving. Dynamic cluster architectures make a better use of the sensors in a WSN and naturally result in improved energy consumption management and network lifetime.
- **Probabilistic and Non-Probabilistic Clustering Algorithms:** This classification based on cluster shape parameters can be used to select the CH. These clustering algorithms are divided into two categories namely. Probabilistic (random or hybrid) and Non-probability (deterministic).

  Most clustering algorithms are known, they can be divided into two main categories. In the probabilistic clustering algorithm for determining the initial CH, a probability assigned to each node. Probabilistic clustering algorithms, beyond the more energy-efficient, often running faster at the convergence and reduce the volume of messages they exchange. In the non-probabilistic clustering algorithms basically criteria (deterministic) more specific for CH selection and cluster formation, take into consideration. These criteria are essentially based on the proximity of adjacent nodes like (connectivity, degree, etc.) and information received from other closely located nodes.

5.3.2 Component of WSN Architecture and Explanation

- Fig. 5.16 shows components of wireless sensor network.

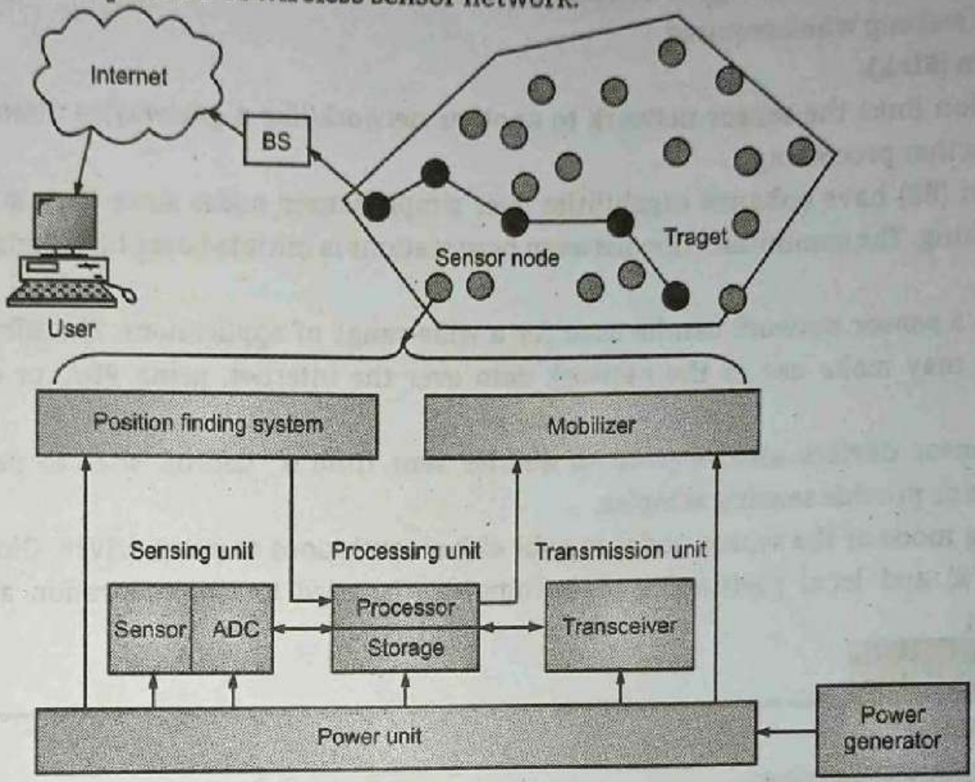


Fig. 5.16: Components of wireless sensor network

- Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed.

1. **Sensor Node:**

- A wireless sensor network consists of hundreds and thousands of low-cost nodes which could either have a fixed location or be randomly deployed to monitor environment.
- Sensors are usually communicate with each other using multi hop approach. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components.
- The individual nodes in a wireless sensor network (WSN) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth.
- After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them.
- Then the onboard sensors start collecting information of interest. The flow of data ends at special node called base station (sink).

2. **Cluster:**

- One of the biggest problem of sensor networks is the power consumption, which is greatly affected by communication between nodes.
- To solve this aggregation points are introduce in network. This reduces the total number of message exchanged between nodes and save some energy.

- Usually, aggregation points are regular nodes that receive the data from neighboring nodes, perform some kind of processing and then forward the filtered data to next hop. Sensor nodes are organize into clusters each cluster having a cluster head as leader. The communication within a cluster must travel through cluster head, which is then forwarded to neighboring cluster head until it reaches its destination i.e. base station.
- Another method to save energy is to set nodes to go to idle (into sleep mode) if the energy is not needed and wakeup when required.

3. Base Station (Sink):

- A base station links the sensor network to another network(like a gateway)to dissimilate the data sense for further processing.
- Base Station (BS) have enhance capabilities over simple sensor nodes since they must do complex data processing. The communication between base stations is initiated over high bandwidth links.

4. End User:

- The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the internet, using PDA, or even a desktop computer.
- Wireless sensor devices also respond to queries sent from a "control site" to perform specific instructions or provide sensing samples.
- The working mode of the sensor nodes may be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms can be used to obtain location and positioning information.

Practice Questions

1. Define MANET.
2. What is MANET Topology.
3. What are the characteristics of MANET.
4. Write any four applications of MANET.
5. What are different types of MANET architecture.
6. What are designing challenges in MANET.
7. Define wireless sensor network.
8. Define mesh networking.
9. Write any four applications of WSN.
10. What is clustering of WSN.
11. What are the characteristics of WSN.
12. Draw and explain block diagram of sensor node.
13. What are different types of WSN architecture.
14. Explain energy efficiency in WSN.
15. Explain design challenges in WSN.
16. Compare MANET, WSN and IOT.
17. Compare WSN and MANET.
18. Explain ISO equivalent protocol layer architecture for WSN.
19. Explain classification of clustering algorithm.
20. Draw component of WSN architecture and explain each term in detail.

✤ ✤ ✤