As per New Syllabus of

GUJARAT TECHNOLOGICAL UNIVERSITY

MOBILE COMPUTING AND WIRELESS COMMUNICATION

Vilas S. Bagad

M.E. (E&Tc), Microwaves
M.M.S. (Information systems)
Faculty, Institute of Telecommunication Management
Ex-Faculty Sinhgod College of Engineering,
Pune

TECHNICAL PUBLICATIONS
An Up-Thrust for Knowledge

Price : ₹ 160 /-
ISBN 978-93-332-1216-8
9 789333 212168

SYLLABUS

Mobile Computing and Wireless Communication - (2170710)

1. **Introduction, Transmission Fundamentals** - Signals for Conveying Information, Analog and Digital Data Transmission, Channel Capacity, TransmissionMedia, Multiplexing

   Communication Networks - LANs, MANs, and WANs, Switching Techniques, Circuit Switching, Packet Switching,

   Protocols and the TCP/IPSuite- The Need for a Protocol Architecture,TheTCP/IP Protocol Architecture,The OSI Model,Internetworking

2. **Cellular Wireless Networks** - Principles of Cellular Networks,First-Generation Analog Second-Generation TDMA Second-Generation CDMA,Third-Generation Systems

   Antennas and Propagation - Antennas, Propagation Modes, Line-of-Sight Transmission, Fading in the Mobile Environment

   Modulation Techniques - Signal Encoding Criteria, Digital Data- Analog Signals, Analog Data-Analog Signals, Analog Data-Digital Signals

   Spread Spectrum - The Concept of Spread Spectrum,Frequency Hopping Spread Spectrum,Direct Sequence Spread Spectrum,Code Division Multiple Access,

   Coding and Error Control - Error Detection, Block Error Correction Codes , Convolutional Codes, Automatic Repeat Request

3. **Multiple Access in Wireless System** - Multiple access scheme, frequency division multiple access, Time division multiple access, code division multiple access, space division multiple access, packet radio access, multiple access with collision avoidance.

   Global system for mobile communication - Global system for mobile communication, GSM architecture, GSM entities, call routing in GSM,PLMN interface, GSM addresses and identifiers, network aspects in GSM,GSM frequency allocation, authentication and security

   General Packet Radio Service(GPRS) - GPRS and packet data network, GPRS network architecture, GPRS network operation, data services in GPRS, Applications of GPRS, Billing and charging in GPRS.

   Wireless System Operations and standards - Cordless Systems, Wireless Local Loop, WiMAX and IEEE 802.16 Broadband Wireless Access Standards

   Mobile IP and Wireless Application Protocol

4. **Wi-Fi and the IEEE 802.11 Wireless LAN Standard** - IEEE 802 architecture, IEEE 802.11 architecture and services, IEEE 802.11 Medium access control, IEEE 802.11 physical layer, Wi-Fi protected access.

5. **Bluetooth** - Radio specification, baseband specification, link manager specification, logical link control and adaption protocol.

6. Android APIs, Android Architecture, Application Framework, The Application components, The manifest file, downloading and installing Android, Exploring the Development Environment, Developing and Executing the first Android application, Working with Activities, The LinearLayout Layout, The RelativeLayout Layout, The ScrollView Layout, The TableLayout Layout, The FrameLayout Layout, Using the TextView, EditText View, Button View, RadioButton, CheckBox, ImageButton, RatingBar, The options Menu, The Context Menu.

Chapter - 6 Android (6 - 1) to (6 - 18)

1 Transmission Fundamentals, Communication, Protocols & TCP/IP

Syllabus

Introduction, Transmission Fundamentals-*Signals for Conveying Information, Analog and Digital Data Transmission, Channel Capacity, Transmission Media, Multiplexing Communication Networks-LANs, MANs, and WANs, Switching Techniques, Circuit Switching, Packet Switching,*

Protocols and the TCP/IP Suite- The Need for a Protocol Architecture, The TCP/IP Protocol Architecture, The OSI Model, Internetworking

Contents

1.1 Signals for Conveying Information

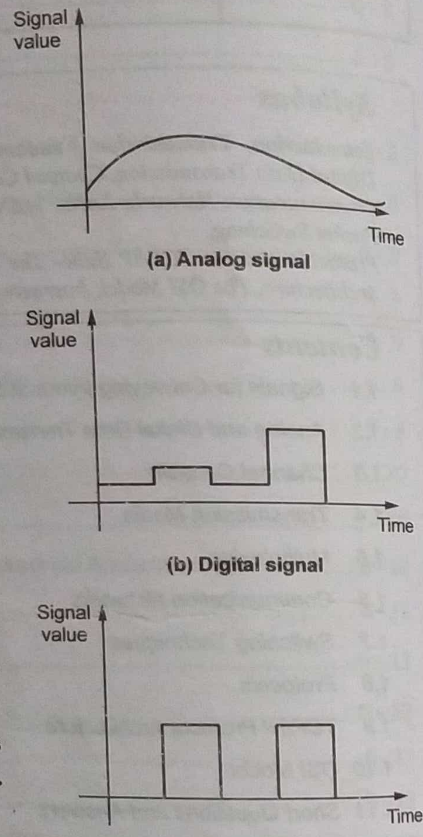
- An electromagnetic signal is a function of time. The electromagnetic signal can also be expressed as a function of frequency it means that the signal consists of components of number of frequencies.

Time domain concepts

- An electromagnetic signal can be either analog or digital. An **analog signal** is one in which the signal intensity varies in a smooth fashion over time. There are no breaks or discontinuities in the signal. Example of analog signal is speech information. The sine wave is the fundamental analog signal.
- The measurement domain where voltage and power are measured as functions of time. Instruments such as oscilloscopes and time interval counters are often used to analyze signals in the time domain.
- A **digital signal** is one in which the signal intensity maintains a constant level for some period of time and then changes to another constant level. The digital signal is represented by binary 1s and 0s.
- The signal in which same signal repeats over the time is called **Periodic signal.** Signal is said to be periodic if :

$$s(t + T) = s(t) \quad -\infty < t < \infty$$

Where T is the period of signal.



(a) Analog signal

(b) Digital signal

(c) (Digital and) binary signal

Fig. 1.1.1 Analog and digital signal

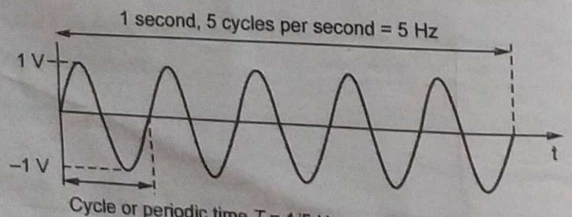

1 second, 5 cycles per second = 5 Hz
1 V
–1 V
t
Cycle or periodic time T = 1/5 Hz = 200 ms

Fig. 1.1.2

- The periodic time or period T in seconds represents the time of one complete cycle :

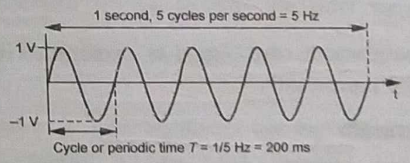
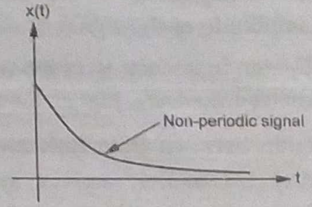
$T = 1/f$ and $f = 1/T$

- Wavelength λ represents the propagation distance in one cycle time, thus,

$$\lambda = c/f = cT$$

where c is the velocity of the signal.

- For a sound wave, the velocity in the air is approximately 346 m/s; for light or radio waves, approximately, c = 300,000 km/sec.

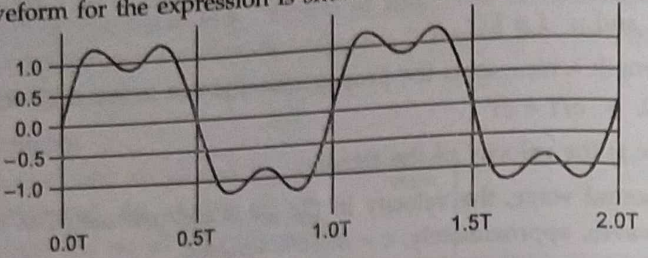
Sr No	Periodic Signal	Aperiodic Signal
1.	A signal which repeats itself after a specific interval of time is called periodic signal.	A signal which does not repeat itself after a specific interval of time is called aperiodic signal.
2.	A signal that repeats its pattern over a period is called periodic signal.	A signal that does not repeats its pattern over a period is called aperiodic signal or non periodic
3.	They can be represented by a mathematical equation.	They cannot be represented by any mathematical equation.
4.	Their value can be determined at any point of time	Their value cannot be determined with certainty at any given point of time.
5.	They are deterministic signals.	They are random signals.
6.	Example : sine, cosine, square, sawtooth etc.	Example : sound signals from radio , all types of noise signals.
7.	 1 second, 5 cycles per second = 5 Hz 1 V –1 V t Cycle or periodic time T = 1/5 Hz = 200 ms	 x(t) Non-periodic signal t

Frequency domain Concept

- In frequency domain voltage and power are measured as function of frequency.
- A spectrum analyzer is often used to analyze signals in the frequency domain. It does so by separating signals into their frequency components and displaying the power level at each frequency.
- The signal consists of sinusoidal components at various frequencies. This frequency-domain description is called the **spectrum**. Consider the expression :

$$S(t) = (4/\pi)\times(\sin(2\pi\, ft)+(1/3)\sin(2\pi\,(3f)t))$$

- The components of this signal are just sine waves of frequencies f and 3f.
- The waveform for the expression is shown in Fig. 1.1.3.



$(4/\pi)\,[\sin(2\pi ft) + (1/3)\sin(2\pi(3f)t)]$

Fig. 1.1.3 Frequency components

Fundamental frequency

- The **fundamental frequency** is defined as the lowest frequency of a periodic waveform. The fundamental frequency is the base frequency such that the frequency of all components can be expressed as its integer multiples; the period of the aggregate signal is the same as the period of fundamental frequency.
- The period of the total signal is equal to the period of the fundamental frequency.
- **Spectrum** is range of frequencies contained in a signal.
- **Absolute bandwidth** is defined as the width of the spectrum.
- **Effective bandwidth** is Narrow band of frequencies containing most of the energy of the signal.
- **DC component** is the component of zero frequency; changes the average amplitude of the signal to non-zero.
- Center frequency is point where bandwidth of a signal is centered. Higher the center frequency, higher the potential bandwidth.

Relationship between Data Rate and Bandwidth

- Any transmitter/receiver system can accommodate only a limited range of frequencies, e.g. the range for FM radio transmission is 88-108 Mhz. This limits the data rate that can be carried over the transmission medium.
- Consider a sine wave of period f. Consider the positive pulse to be binary 1 and the negative pulse to be binary 0. Add to it sine waves of period 3f, 5f, 7f, . . .
- The resultant waveform starts to approximate a square wave. Frequency components of a square wave with amplitude A and –A can be expressed as-

$$s(t) = A \times 4\pi \times \sum_{k\,\text{odd},\, k=1}^{\infty} \frac{\sin(2\pi\, kft)}{k}$$

- This waveform has infinite number of frequency components and infinite bandwidth.
- Peak amplitude of k^{th} frequency component is 1/k so most of the energy is concentrated in the first few frequencies. Limiting the bandwidth to only the first few frequencies gives a shape that is reasonably close to square wave.
- Digital transmission system capable of transmitting signals with a bandwidth of 4 Mhz.

Case I : Approximate square wave with a waveform of first three sinusoidal components.

$$\frac{4}{\pi}\left[\sin(2\pi\, ft) + \frac{1}{3}\sin(2\pi(3f)t) + \frac{1}{5}\sin(2\pi(5f)t\right]$$

If $f = 10^6$ cycles per seond, or 1 MHz, the bandwidth of the signal.

$$s(t) = \frac{4}{\pi}\left[\sin(2\pi \times 10^6 \times t) + \frac{1}{3}\sin(2\pi \times 3 \times 10^6 \times t) + \frac{1}{5}\sin(2\pi \times 5 \times 10^6 \times t)\right]$$

is $(5\times10^6) - 10^6 = 4$ MHz.

For f = 1 MHz, period of fundamental frequency is $T = \frac{1}{10^6} = 10^{-6} = 1\ \mu s$

If the waveform is a bit string of 1's and 0's, one bit occurs every 0.5 μs, for a data rate of 2×10^6 bps or 2 Mbps.

Case II : Assume a bandwidth of 8 MHz and f = 2 MHz; this gives us the signal bandwidth as

$$(5\times2\times10^6) - (2\times10^6) = 8 \text{ MHz}$$

But $T = \frac{1}{f} = 0.5\ \mu s$, so that the time for one bit is 0.25 μs giving a data rate of 4 Mbps. Other things being equal, doubling of bandwidth doubles the potential data rate.

Case III : Let us represent the signal by the first two components of the sinusoid as,

$$\frac{4}{\pi}\left[\sin(2\pi ft) + \frac{1}{3}\sin(2\pi(3f)t)\right]$$

Assume that f = 2 MHz and $T = \frac{1}{f} = 0.5\ \mu s$ so that the time for one bit is 0.25 μs giving a data rate of 4 Mbps. Bandwidth of the signal is,

$$(3\times2\times10^6) - (2\times10^6) = 4 \text{ MHz}$$

- A given bandwidth can support various data rates depending on the ability of the receiver to discern the difference between 0 and 1 in the presence of noise and other impairments.
- Any digital waveform has infinite bandwidth because -

1. The transmission system limits the waveform as a signal over any medium.
2. For any given medium, cost is directly proportional to bandwidth transmitted.
3. Signal of limited bandwidth is preferable to reduce cost.
4. Limiting the bandwidth creates distortions making it difficult to interpret the received signal.

1.2 Analog and Digital Data Transmission

- Analog signal corresponds to continuous and digital corresponds to discrete signal.
- Data is defined as entities that convey information or meaning.
- **Signal** is electric or electromagnetic representations of **data**.
- **Signaling** is a process of physical propagation of signal along suitable medium.
- **Transmission** is defined as communication of data by propagation and processing of signals.

Analog and Digital Signaling

- An **analog signal** is a continuously varying electromagnetic wave that can propagated over a variety of media.
- The selection of media is depending on frequency. Examples of transmission media are copper wire media (twisted pair and coaxial cable); fiber optic cable and atmosphere or space propagation (wireless).
- A **digital signal** is a sequence of voltage pulses that may be transmitted over a copper wire medium; for example, a constant positive voltage level may represent binary 0 and a constant negative voltage level may represent binary.

Sr No	Analog signal	Digital signal
1.	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
2.	Denoted by sine waves	Denoted by square waves
3.	Analog signal processing can be done in real time and consumes less bandwidth.	There is no guarantee that digital signal processing can be done in real time and consumes more bandwidth to carry out the same information.
4.	Stored in the form of wave signal.	Stored in the form of binary bit.
5.	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
6.	Analog instrument draws large power.	Digital instrument draws only negligible power.
7.	Examples : Human voice in air, analog electronic devices.	Examples : Computers, CDs, DVDs, and other digital electronic devices.

1. **Digital data/Analog signals**

- It is necessary to convert digital data to analog signal. One such device is a modem to translate between bit-serial and modulated carrier signals.
- To send digital data using analog technology, the sender generates a carrier signal at some continuous tone (e.g. 1-2 kHz in phone circuits) that looks like a sine wave. Several techniques are used to encode digital data into analog signals. Resulting bandwidth is centered on the carrier frequency.

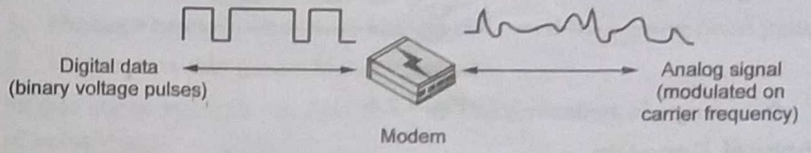


Fig. 1.2.1

2. **Analog data/Analog signals**

- It is transmission of analog data in a similar manner with amplitude, phase and frequency-modulated waves.

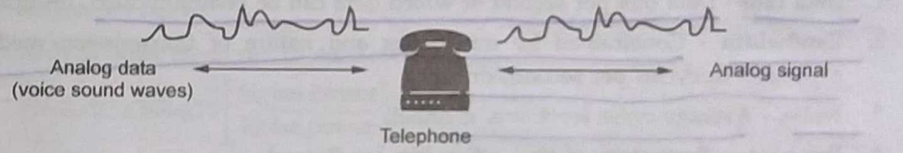


Fig. 1.2.2

- Two reasons for this form of transmission :
  a) Transmission media may need to use a higher frequency than that used by the data (such as voice).
  b) Modulation permits frequency-division multiplexing.

3. **Digital data/Digital signals**

- A simple encoding method is to use constant voltage levels for a "1" and a "0". Can lead to long periods where the voltage does not change.

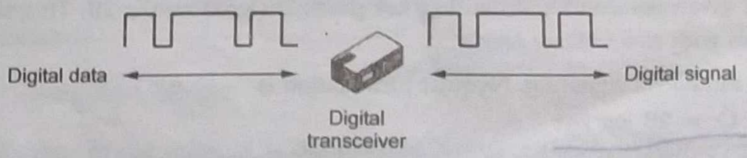


Fig. 1.2.3

4. **Analog data/Digital signals**

- Although most local loops are analog, end offices increasingly use digital circuits for inter-trunk lines. A codec (coder/decoder) is a device that converts an analog signal into a digital signal.
- To convert analog signals to digital signals, many systems use Pulse Code Modulation (PCM) :

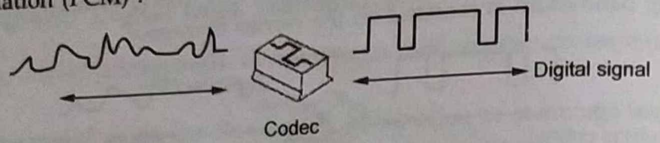


Fig. 1.2.4

1.3 Channel Capacity

Maximum rate at which data can be transmitted over a communication path or channel is called **channel capacity.**

- The channel capacity depends on four factors :

1. **Data rate** - Data bits per second at which data can be communicated. (in bps)
2. **Bandwidth** - Constrained by transmitter and nature of transmission medium, expressed in cycles per second, or Hz.
3. **Noise** - Average noise level over channel.
4. **Error rate** - Percentage of time when bits are flipped.

- Bandwidth is proportional to cost, for digital data, it is desirable to get as high a data rate as possible within a limit of error rate for a given bandwidth.

1.3.1 Nyquist Bandwidth

- There is limitation on data rate for a noise free channel. Data rate equals to channel bandwidth.
- If the rate of signal transmission is 2B, then a signal with frequencies no greater than B is sufficient to carry the signal rate.
- For a given bandwidth B, the highest possible signal rate is 2B. This is true for signals with two voltage levels.
- With multilevel signaling, Nyquist formulation is

$$C = 2B \log 2M$$

where M is the number of discrete signal elements or voltage levels.

- For a given bandwidth, data rate can be increased by increasing the number of different signal elements. Value of M is practically limited by noise and other impairments on transmission line.

1.3.2 Shannon Capacity Formula

- Nyquist formula gives the relationship between bandwidth and data rate.
- Noise can corrupt bits of data :

1. Shorter bits imply that more bits get corrupted by a given noise pattern.
2. Higher data rate means higher error rate.

- Higher signal strength can lead to better discrimination of signal in the presence of noise.

Signal-to-Noise (SNR) ratio

- SNR is defined as ratio of power in signal to the power in noise present at a particular point in the noise.
- SNR is typically measured at the receiver to process the signal and eliminate unwanted noise.
- SNR is often measured in decibels

$$(\text{SNR})\text{dB} = 10\log 10 \left[\frac{\text{Signal Power}}{\text{Noise power}}\right]$$

- SNR expresses the amount by which the intended signal exceeds the noise level.
- High SNR implies a high quality signal while low snr indicates the need for repeaters.
- SNR sets the upper bound on achievable data rate.
- Maximum channel capacity C, in bps, is given by :

$$C = B \log 2\ (1 + \text{SNR})$$

where B is the bandwidth of the channel in Hz

- Shannon formula gives the maximum possible capacity assuming only white noise; it does not take into account the impulse noise, delay distortion, and attenuation.

1.4 Transmission Media

- The transmission medium is the physical path between transmitter and receiver. Transmission media is also called **Communication channel.**
- The transmission media that are used to convey information can be classified as guided or unguided. Guided media provide a physical path along which the

signals are propagated; these include twisted pair, coaxial cable, and optical fiber. Unguided media employ an antenna for transmitting through air, vacuum or water.

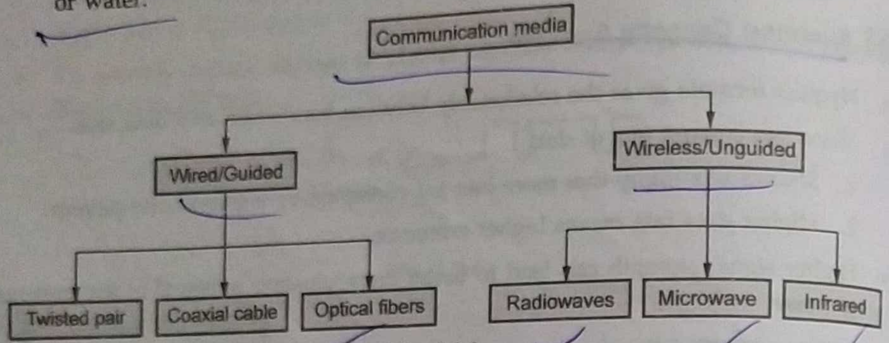


Fig. 1.4.1

- The characteristics and quality of a data transmission are determined both by the characteristics of the medium and the characteristics of the signal. In the case of guided media, the medium itself is more important in determining the limitations of transmission.
- The data transmission capabilities of various medias vary differently depending upon the various factors. These factors are :

1. **Bandwidth** - It refers to the data carrying capacity of a channel or medium. Higher bandwidth communication channels support higher data rates.
2. **Radiation** - It refers to the leakage of signal from the medium due to undesirable electrical characteristics of the medium.
3. **Noise Absorption** - It refers to the susceptibility of the media to external electrical noise that can cause distortion of data signal.
4. **Attenuation** - It refers to loss of energy as signal propagates outwards. The amount of energy lost depends on frequency. Radiations and physical characteristics of media contribute to attenuation.

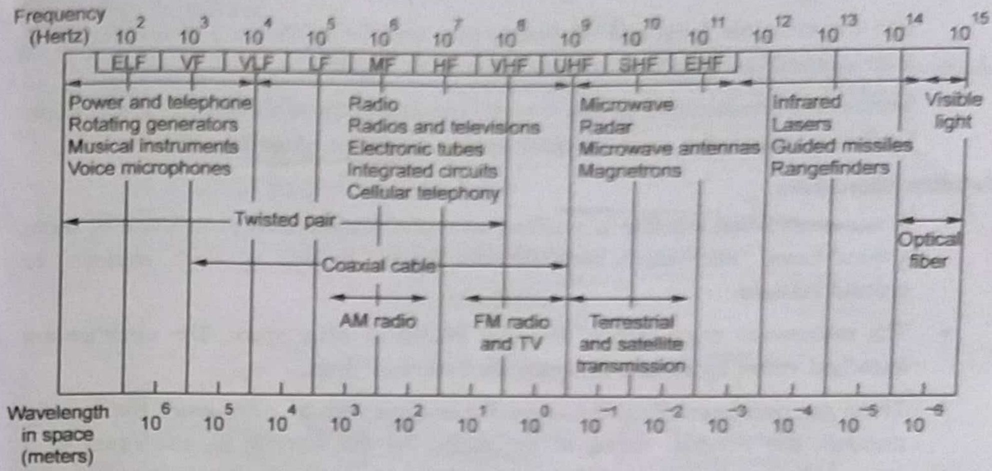
Electromagnetic spectrum

- Electromagnetic Spectrum for various communication media is shown in Fig. 1.4.2.

(See Fig. 1.4.2 on next page)

Microwave Transmission

- It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.



ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

Fig. 1.4.2

- There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Terrestrial Microwave

- A primary use for terrestrial microwave systems is in long-haul telecommunications service, as an alternative to coaxial cable or optical fiber.
- For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna. The signal received by an antenna can be converted

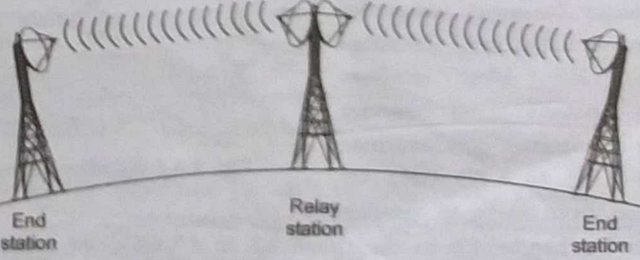


Fig. 1.4.3 Terrestrial microwave

into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world.

- Microwave transmission covers a major portion of the electromagnetic spectrum. Common frequencies used for transmission are in the range 2 to 40 GHz.

Satellite Microwave

- A communication satellite is a microwave relay station used to link two or more ground-based microwave transmitter/receivers, known as earth stations, or ground stations.
- The microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.
- These are positioned 3600 km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.
- Satellite communication takes place through the propagation of focused and directed electromagnetic (EM) waves.
- Since both received and transmitted waves are simultaneously present at very different power levels, in a satellite, both frequency separation and EM field polarization are used to decouple the channels.
- The term link refers to a path used to communicate with the satellite (and is sometimes used to refer to the communication itself) :
  1. Uplinks transmit signals from a ground station to the satellite.
  2. Downlinks transmit signals from the satellite to a ground station.
  3. Cross-links transmit signals from satellite to sateiiite.
- The optimum frequency range for satellite transmission is in the range 1 to 10 GHz. Most satellites providing point-to-point service today use a frequency bandwidth in the range 5.925 to 6.425 GHz for transmission from earth to satellite (uplink) and a bandwidth in the range 3.7 to 4.2 GHz for transmission from satellite to earth (downlink).

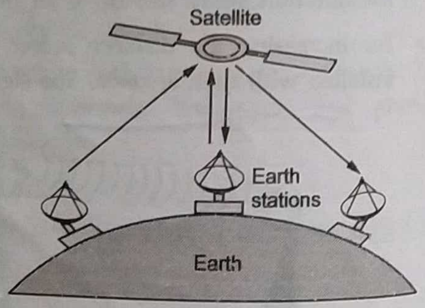


Fig. 1.4.4 Satellite microwave

1.5 Multiplexing

- Multiplexing is a technique that allows the simultaneous transmission of multiple signals across a single data link. There are three categories of multiplexing.
  1. Frequency-Division Multiplexing (FDM)
  2. Time Division Multiplexing (TDM)
  3. Wavelength Division Multiplexing (WDM)

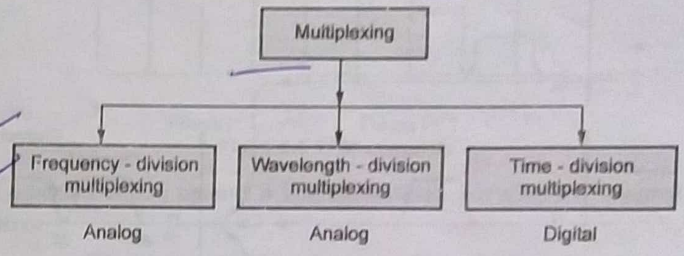

Multiplexing
Frequency - division multiplexing
Wavelength - division multiplexing
Time - division multiplexing
Analog
Analog
Digital

Fig. 1.5.1 Multiplexing types

1.5.1 Frequency-Division Multiplexing (FDM)

- Frequency-Division Multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. Example : multiplexing 12 analogue voice channels (4 kHz nominal bandwidth) into a link with bandwidth equal to 48 kHz.

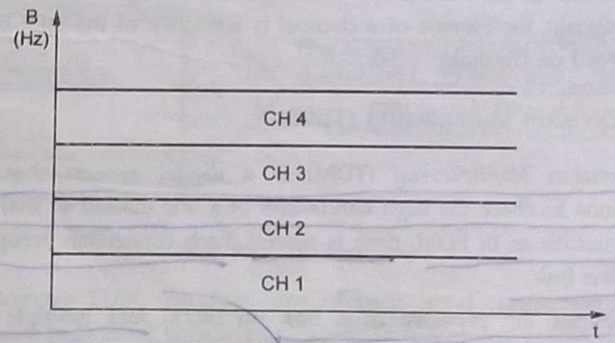
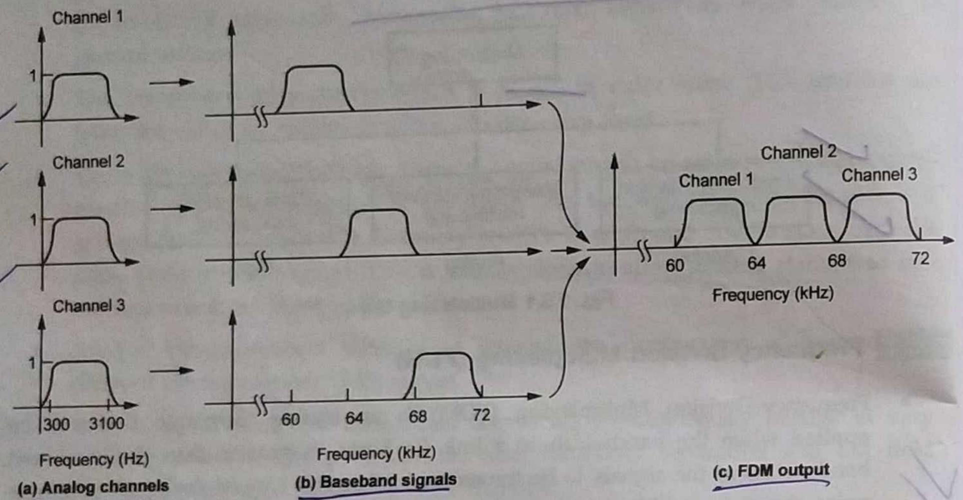


Fig. 1.5.2 FDM channels

- In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link.

- Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies.
- Fig. 1.5.3 shows FDM process.



(a) Analog channels (b) Baseband signals (c) FDM output

Fig. 1.5.3 FDM process

- Transmission in all channels is simultaneous, on separate frequency bands (for digital signals, the bit rate of a channel is a fraction of the total bit rate that may be achieved on the link)

1.5.2 Time Division Multiplexing (TDM)

- Time-Division Multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a line instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link.
- TDM divides the capacity of a link (in bit/s) into multiple channels using temporal interleaving - the channels occupy different (non overlapping) time slots. Fig. 1.5.4 shows TDM channels.
- The basic form of TDM is Synchronous Time Division Multiplexing (STM) - fixed size time slots allocated to each channel repeat periodically and time slots in the same cycle constitute a frame. Example : for a frame made up of 32 time slots

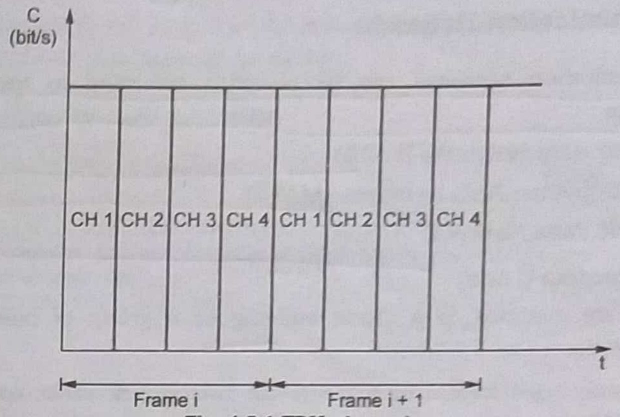


Fig. 1.5.4 TDM channels

with a period of 125 μs and 8 bits transmitted per slot, the channel capacity is 64 kbit/s

- A channel is identified by the position of the slot it occupies in the frame (position multiplexing), which requires a mechanism for identifying the start of a frame (frame synchronization).
- Each flow is transmitted on the multiplexed link at the link rate and a conversion to the original rate occurs at the demultiplexer - the flow suffers a fixed delay (that corresponds to the time to access its slot).

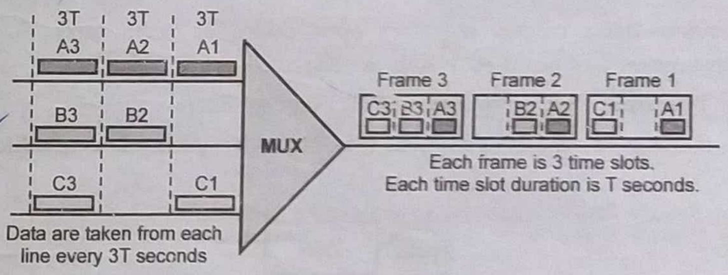

3T
3T
3T
A3
A2
A1
B3
B2
C3
C1
MUX
Frame 3
Frame 2
Frame 1
C3
B3
A3
B2
A2
C1
A1
Each frame is 3 time slots.
Each time slot duration is T seconds.
Data are taken from each line every 3T seconds

Fig. 1.5.5 TDM process

- In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot.
- A round of data units from each input connection is collected into a frame. If we have n connections, a frame is divided into n time slots and one slot is allocated for each unit, one for each input line.

1.6 Communication Networks

- Communication networks can be classified according to their geographical coverage :
  1. Local Area Networks (LANs)
  2. Metropolitan Area Networks (MANs)
  3. Wide Area Networks (WANs)

Local Area Networks (LANs)

- LANs are confined to a single building or a group of building within an organization.
- Commonly used transmission media are twisted pair cable, coaxial cables and optical fibers.

Metropolitan Area Networks (MANs)

- MANs are used to interconnect computers within metropolitan city.
- Communication medias are shielded lines, optical fibers, radio links.
- Broadband capability provides data, voice and video transmission i.e. MANs are multimedia networks.
- Synchronous optical networks (SONET) are designed to operate at high speeds.

Wide Area Networks (WANs)

- Intercity, intercountry and intercontineutal networks are known as WANs.
- Communication medias are fiber optic cables or radio links. According to transmission facilities used WANs are classified as -
  a) Terrestrial Data Networks (TDNs) : Optical fibers.
  b) Satellite Based Data Networks (SBDNs) : Geosynchronous satellite.

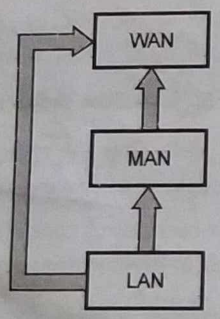


Fig. 1.6.1 Data network hierarchy

- A global network can be formed by interconnection of LANs, MANs and WANs. Fig. 1.6.1 shows data network hierarchy.

1.6.1 Comparison of LAN and WAN

	LAN	WAN
Definition :	LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, schools, or group of buildings.	WAN (Wide Area Network) is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries over a long distance.
Components :	layer 2 devices like switches, bridges. layer1 devices like hubs , repeaters.	Layers 3 devices Routers, Multi-layer Switches and Technology specific devices like ATM or Frame-relay Switches etc.
Data transfer rates :	LANs have a high data transfer rate.	WANs have a lower data transfer rate as compared to LANs.
Technology :	Tend to use certain connectivity technologies, primarily Ethernet and Token Ring.	WANs tend to use technology like MPLS, ATM, Frame Relay and X.25 for connectivity over the longer distances.
Connection :	one LAN can be connected to other LANs over any distance via telephone lines and radio waves.	Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.
Speed :	high speed (1000 mbps)	less speed (150 mbps)
Maintenance costs :	Because it covers a relatively small geographical area, LAN is easier to maintain at relatively low costs.	Maintaining WAN is difficult because of its wider geographical coverage and higher maintenance costs.
Fault tolerance :	LANs tend to have less problems associated with them, as there are a smaller amount of systems to deal with.	WANs tend to be less fault tolerant. as it consists of a large amount of systems there is a lower amount of fault tolerance.
Data transmission error :	Experiences fewer data transmission errors.	Experiences more data transmission errors as compared to LAN
Ownership :	Typically owned, controlled and managed by a single person or organization.	WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management over long distances.

1.7 Switching Techniques

- **Switching** is process to forward packets coming in from one port to a port leading towards the destination. Long distance transmission is typically done over a network of switched nodes.
- The switching devices are called **nodes**. Some nodes connect to other nodes and some are connected to some stations.
- The switching performed by different nodes can be categorized into the following three types :

1. Circuit Switching 2. Packet Switching 3. Message Switching

1.7.1 Circuit Switching

- In circuit switched networks, an electrical path is established between the source and destination before data transfer.
- The electrical path may be realized via physical wires, radio or satellite links.
- The path established is dedicated for the entire period of transmission. No other user can access the path. The connection is released only when signalled by communicating devices.
- Example of circuit switched data network is PSTN.

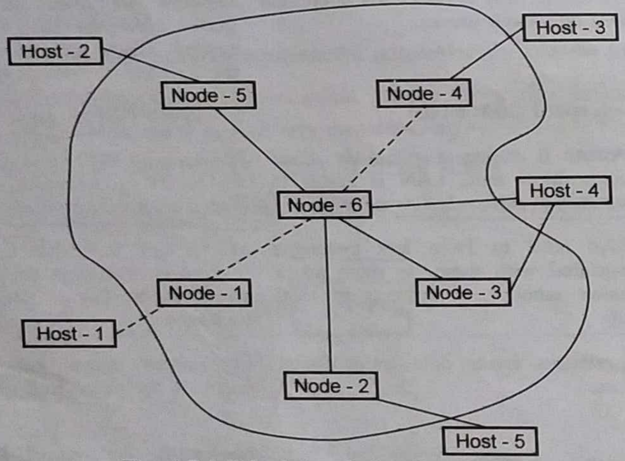


Fig. 1.7.1 Principle of circuit switching

- Host - 1 wants to communicate to Host - 3, a connection request is made to switching node N1, the node N1 selects a suitable neighbouring node based on routing algorithm (Node - 6). Now node - 6 selects a suitable forward path until electrical path between Host - 1 and Host - 3 is established.

Advantages of circuit switching

1. Real-time transfer of voice signals.
2. Technology is mature.
3. Lowest end to end delay.

Disadvantages of circuit switching

1. Comparatively high cost of switch.
2. Lower system utilization.
3. Call may be lost in busy network.

1.7.2 Packet Switching

- It is a form of store and forward network. The message is split into number of packets of fixed size and these packets are transmitted in store and forword (S & F) format.
- Each packet transmission is independent of others. The packet may travel via different route with different delays. At destination host, these packets are reassembled.
- Each packet contains destination host id, source id, message id and packet id.

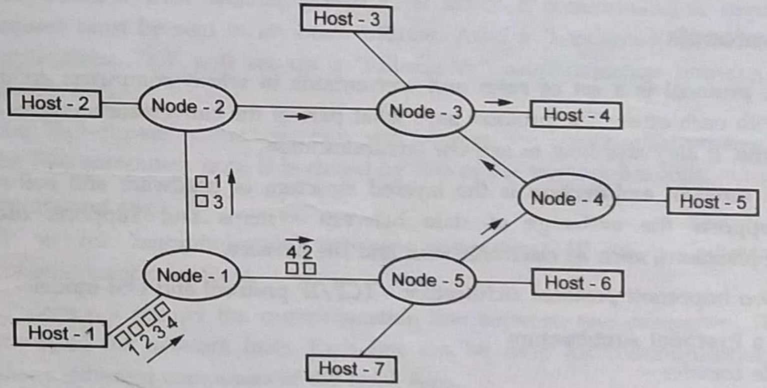


Fig. 1.7.2 Packet switched network

- Host - 1 wants to send message to Host - 4, the message is divided into packets 1, 2, 3 and 4. These packets may take different path and at destination they may arrive at out of sequence. It is the responsibility of network to resequence the packets before delivery to the destination.

- Packet network offers forms at services.

  1. Datagram service 2. Virtual circuit service.

Advantages of packet switching

1. Packet switching is cost effective, because switching devices do not need mas amount of secondary storage.
2. Packet switching offers improved delay characteristics, because there are n long messages in the queue (maximum packet size is fixed).
3. Packet can be rerouted if there is any problem, such as, busy or disabled link
4. The advantage of packet switching is that many network users can share same channel at the same time. Packet switching can maximize link efficie by making optimal use of link bandwidth.

Disadvantages of packet switching

1. Protocols for packet switching are typically more complex.
2. It can add some initial costs in implementation.
3. If packet is lost, sender needs to retransmit the data. Another disadvantag that packet-switched systems still can't deliver the same quality as dedica circuits in applications requiring very little delay - like voice conversations moving images.

1.8 Protocols

- A **protocol** is a set of rules and conventions in which computers communi with each other. The protocol says what part of the conversation comes at wh time. It also says how to end the communication.
- A **protocol architecture** is the layered structure of hardware and software supports the exchange of data between systems and supports distrib applications, such as electronic mail and file transfer.
- Two important protocol architecture - TCP/IP protocol and OSI model.

Need for a Protocol Architecture

1. File transfer -
   a. Source must activate communication Path or inform network of destinat
   b. Source must check destination is prepared to receive.
   c. File transfer application on source must check destination file manage system will accept and store file for his user.
   d. May need file format translation.
2. Task broken into subtasks
3. Implemented separately in layers in stack.

4. Functions needed in both systems
5. Peer layers communicate

1.9 TCP/IP Protocol Architecture

- TCP/IP stands for Transmission Control Protocol / Internet Protocol.TCP/IP is the communication protocol for communication between computers on the Internet.TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them.
- The TCP/IP standard consists of several protocols for handling data communication :
  1. TCP (Transmission Control Protocol) communication between applications
  2. UDP (User Datagram Protocol) simple communication between applications
  3. IP (Internet Protocol) communication between computers
  4. ICMP (Internet Control Message Protocol) for errors and statistics
  5. DHCP (Dynamic Host Configuration Protocol) for dynamic addressing

CP Uses a Fixed Connection

- TCP is for communication between applications. If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a "handshake" between the two applications, TCP will set up a "full-duplex" communication between the two applications.
- The "full-duplex" communication will occupy the communication line between the two computers until it is closed by one of the two applications.

' is Connection-Less

- IP is for communication between computers. IP is a "connection-less" communication protocol.
- IP does not occupy the communication line between two computers. IP reduces the need for network lines. Each line can be used for communication between many different computers at the same time.
- With IP, messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet.
- IP is responsible for "routing" each packet to the correct destination.

CP/IP

- TCP/IP is TCP and IP working together.TCP takes care of the communication between your application software (i.e. your browser) and your network software.

- TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive.
- IP takes care of the communication with other computers.
- IP is responsible for sending the packets to the correct destination

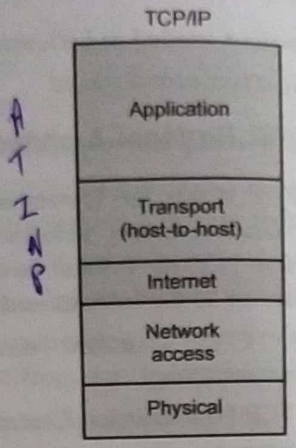


Fig. 1.9.1 TCP/IP reference model

1.10 OSI Model

- ISO-OSI refers to International Standardisation Organisation - Open sys interconnection. ISO-OSI standard describes a method of interconnection architecture for data communication network.
- ISO-OSI standard specifies layered communication architecture also the method of interconnection of systems, subsystems and layers.

System : One or more standalone computers.

Subsystems : A part of system that is logically independent.

Layer : Composed of subsystems of same rank of all the interconnected systems.

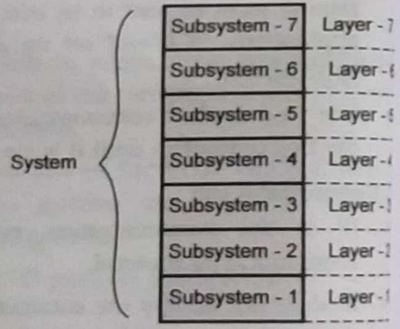


Fig. 1.10.1 Systems, subsystems and layers in ISO-OSI

- Fig. 1.10.1 illustrates systems, subsystems and layers in ISO-OSI model.
- The function in a layer performed by hardware systems or software packages known as **entities.**
- The data exchange between peer entities takes place in the form of protocol d units (PDUs). Fig. 1.10.2 shows structure of PDU.

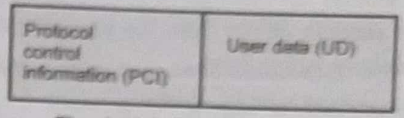


Fig. 1.10.2 Structure of PDU

- Data exchange between entities of adjacent layers i.e. between layer N and layer N-1, takes place in the term of interface data units (IDUs). Fig. 1.10.3 shows structure of IDU.

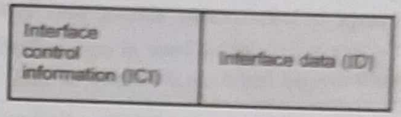


Fig. 1.10.3 Structure of IDU

1.10.1 Link-to-Link Layers

- ISO-OSI reference model has seven layers as shown in Fig. 1.10.4. The first three layers i.e. physical, data link and network layer, the communication proceeds on a link-to-link basis.

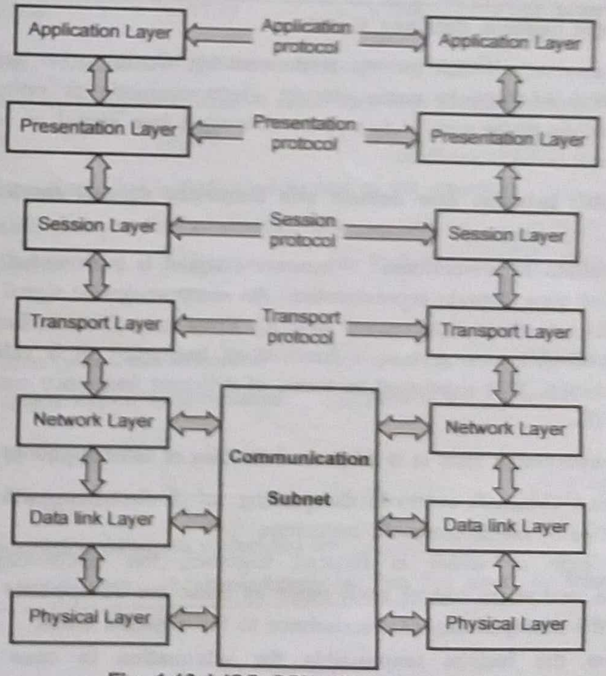


Fig. 1.10.4 ISO OSI reference model

- In link-to-link basis services obtain from the immediate lower layer and provide services to the immediate upper layer.
- OSI services are categorized into two forms -

1. Connection oriented services
2. Connection less services

- Peer entities of OSI layers communicate using peer protocols.
- **Protocols** are strict procedures and sequence of actions to be followed in order to achieve orderly exchange of information among peer entities.

1.10.2 End-to-End Layers

- Layers 4 to 7 of ISO-OSI reference model (i.e. transport, session, presentation application layers) communicate with peer entities in the end systems.
- While communication among these layers there are no intermediate system hence layers 4 to 7 are called **end-to-end layers.**

1.11 Short Questions and Answers

Q.1 Distinguish between data and signal.

Ans : Data is an entity, which conveys some meaning. On the other hand, the signal is a representation of data in some electric, electromagnetic or optical form. So, whenever data needs to be sent, it has to be converted into signal of some form for transmission over a suitable medium.

Q.2 Distinguish between time domain and frequency domain representation of a signal.

Ans : Time Domain Representation : Whenever a signal is represented as a function of time, it is called time domain representation. An electromagnetic signal can be either continuous or discrete. It is represented as s (t). Frequency Domain Representation : Whenever a signal is represented as a function of frequency, it is called frequency domain representation. It is expressed in terms of different frequency components and represented as s (f).

Q.3 What is crosstalk? How is it minimized in case of twisted-pair of wire?

Ans : **Crosstalk :** Crosstalk refers to the picking up of electromagnetic signals from other adjacent wires by electromagnetic induction.

When a pair of wires is twisted together, the electromagnetic signals generated by the two wires cancel each other as these are of opposite polarity. This helps to reduce the susceptibility of interference to the adjacent wires.

Q.4 What are the factors responsible for attenuation in case of terrestrial microwave communication?

Ans. : Attenuation due to distance is 10 log (4πd/λ)2. Factors responsible for attenuation are given below :

1. Distance - Attenuation is more if distance increases.
2. Wavelength - Attenuation is less if wavelength is longer. (i.e. high frequency components are attenuated more than the low frequency component).
3. Rainfall - Attenuation is less if there is no rain.

Q.5 What equipments are used to visualize electrical signals in time domain and frequency domain?

Ans : Cathode Ray Oscilloscope is used to visualize electrical signals in time domain and Spectrum Analyzer used to visualize electrical signals in frequency domain.

1.12 Multiple Choice Questions

Q.1 The sharing of a medium and its link by two or more devices is called _______.

a Fully duplexing b Multiplexing c Both a and b d None of the mentioned **[Ans. : b]**

Q.2 Which multiplexing technique transmits digital signals ?

a FDM b TDM c WDM d None of the mentioned **[Ans. : b]**

Explanation : FDM and WDM are used in analog signals.

Q.3 If there are n signal sources of same data rate than TDM link has _______ slots.

a n b n/2 c n*2 d 2^n **[Ans. : a]**

Explanation : Each slot is dedicated to one of the source.

Q.4 In TDM, slots are further divided into _______.

a Seconds b Frames c Packets d None of the mentioned **[Ans. : b]**

Q.5 OSI stands for _______.

a open system interconnection b operating system interface

c optical service implementation d none of the mentioned **[Ans. : a]**

Q.6 The OSI model has ___ layers.

a 4 b 5 c 6 d 7 **[Ans. : d]**

Q.7 Transmission data rate is decided by _____.

a network layer b physical layer c data link layer d transport layer **[Ans. : b]**

❑❑❑

2.1 Cellular Wireless Networks

- The potential of communication without wires have grown tremendously due to invention and development of sophisticated radio equipments. The mobile radio systems are now becoming so popular for both business and domestic use.
- The available frequency bands are becoming saturated without meeting even a fraction of the increased demand. The conventional land mobile system suffers from the problem of -
  1. Limited service capability
  2. Poor service performance
  3. Inefficient frequency spectrum utilization
  4. Spectral congestion in mobile radio environment.
- All above problems can be solved in cellular mobile telephone system.

2.1.1 Principle of Cellular Networks

- A **cellular system** is a combination of a modulation and multiple access techniques, this method is equally applicable to both analog and digital systems. **Cellular radio** is a technique that was developed to increase the capacity available for mobile radio telephone service.
- Cellular systems are complex but a much more efficient. It includes several disciplines of engineering and has taken much enterprise and development to assemble into global systems. Prior to the introduction of cellular radio, mobile radio telephone service was only provided by a high-power transmitter/receiver. Also, a typical system supported about 25 channels with an effective radius of about 80 km.
- Cellular radio requires combination of many large scale technology e.g. HF semiconductor technologies, radio transmission planning and global fixed telecommunications networks.
- The way to increase the capacity of the system is to use lower-power systems with shorter radius and to use numerous (many) transmitters/receivers.

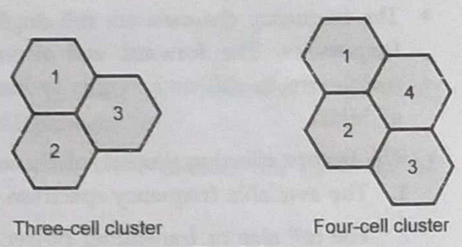
2.1.1.1 Cellular Network Organization

- The essence of a cellular network is the use of multiple low-power transmitters, typically 100 W or less, as the range of transmitter is small, an area can be divided into cells, each one served by its own antenna.

- Each cell is allocated a band of frequencies and is served by a base station, consisting of transmitter, receiver, and control unit.
- Adjacent cells are assigned different frequencies to avoid interference or crosstalk. But, cells sufficiently distant from each other can use the same frequency band.
- In cellular systems, improved spectral efficiency and ability to handle heavy traffic demands can be achieved by frequency reuse and cell splitting techniques.
- Frequency reuse refers to the use of radio channels on the same carrier frequency to cover different areas which are separated from one another by a sufficient distance so that co-channel interference is not objectionable.
- Cell splitting is further dividing a cell into smaller cells a set of channel frequencies is reused more often, leading to a higher spectral efficiency.
- Higher spectral efficiency leads to more subscribers, cheaper equipment due to mass production, low call charges and, overall lower cost per subscriber.
- Examples of analog cellular mobile radio systems are -
  1. AMPS (Advanced Mobile Phone System) in USA,
  2. TACS (Total Access Cellular System) in UK,
  3. NAMTS (Nippon Advanced Mobile Telephone System) in Japan.

2.1.1.2 Cellular Concept

- The overall service area is divided into small cell, ideally with no gaps or overlaps, each cell being served by its own base station and a set of channel frequencies. The power transmitted by each station is controlled in such a way that the local mobile stations in the ~ell are served, while co-channel interference, in the cells using the same set of radio channel frequencies is kept minimum.
- As shown in Fig. 2.1.1 the cells are hexagons with the repeater and base station at the centre. The N cells which collectively use the complete set of available frequencies is called a **cluster**.



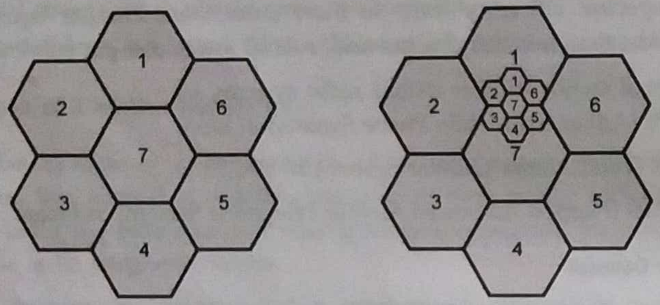
Three-cell cluster

Four-cell cluster

Fig. 2.1.1

- Cell sizes are made smaller at the centre of the city or area of occupation of most subscribers.
- Cells are arranged in clusters. Only certain clusier sizes are possible, principally due to geometry of a hexagon and the allowable cluster sizes of 3, 4, 7 and 12 are shown by way of illustration.

- The hexagon shape permits easy and manageable analysis of a cellular system. The actual radio coverage of a cell is known as **footprint**. The footprint of cell is determined by field measurements or propagation prediction models.
- The hexagonal cells fit together to form a honey comb pattern. Fig. 2.1.2 shows seven cell honey comb pattern or seven cell cluster.
- The hexagonal shape of cell ensures the most effective transmission but in reality the antenna patterns will not achieve this pattern, the cells more likely takes the circular pattern with some overlap.
- When planning a system the aim must be to achieve the maximum use of the available radio spectrum. Also there must be low interference, good quality speech and an acceptable grade of service.



(a) Honey comb pattern or seven cell cluster

(b) Two sizes of cell

Fig. 2.1.2 The concept of cell

- The frequency channels are full duplex hence each conversation requires a pair of frequencies. The forward and reverse directions from the base station to the mobile are to different frequency band and the two frequencies are separated by 45 MHz.
- The factors affecting number of channels in a particular area :
  1. The available frequency spectrum.
  2. The cell size or transmitter power.
  3. The reduction in the quality of the link that can be tolerated due to co-channel interference.
- The normal maximum number of channels operating in a cell is limited to 120 and this occurs in places where the traffic is highest. The capacity of a system in an area is determined by the number of channels in a cell and the cell size.

- The number of simultaneous users is given by expression :

$$n = \frac{m\,(W / N)}{B}$$

Where,

W is total available spectrum,

B is bandwidth needed per user,

N is frequency reuse factor,

m is number of cell required to cover an area.

- Above expression indicates the capacity of network can be increased by :
  i) Increasing m
  ii) Decreasing frequency reuse factor

2.1.1.3 Cellular Hierarchy

- Hierarchical cellular infrastructures of different sizes are used in cellular network because of following reasons :

i) To extend the coverage to the areas those are difficult to cover by a large cell.

ii) To increase the capacity of the network for those areas that has a higher density of users.

iii) To provide coverage for specific application

- For deployment of cellular network numbers of cell sizes are used to provide a comprehensive coverage supporting traffic fluctuations in different geographic areas and supporting a variety of applications.
- Different cell sizes are defined as following.

1. Femtocells

- Femtocells are the smallest unit of hierarchy used for connection of personal equipment such as laptops and cellular telephones.
- The femtocells cover only few meters where these devices are used within physical range of users.

2. Picocells

- Picocells are the small cells inside a building that support local indoor networks. For example, wireless LANs, Wi-Fi networks.
- The size of these networks is in the range of a few tens of meters.

3. Microcells

- The microcells cover the interiors of streets and its antenna is located at the heights lower than the rooftop of the building.

- The microcell covers range of few hundreds of meter. It is used for personal communication systems.

4. Macrocells

- Macrocells cover metropolitan areas and its antennas are mounted above the rooftop of the buildings in the coverage area.
- The macrocells cover areas on the order of several kilometres.

5. Megacells

- Megacells cover nationwide areas with satellites. It usually covers ranges of hundreds of kilometers.

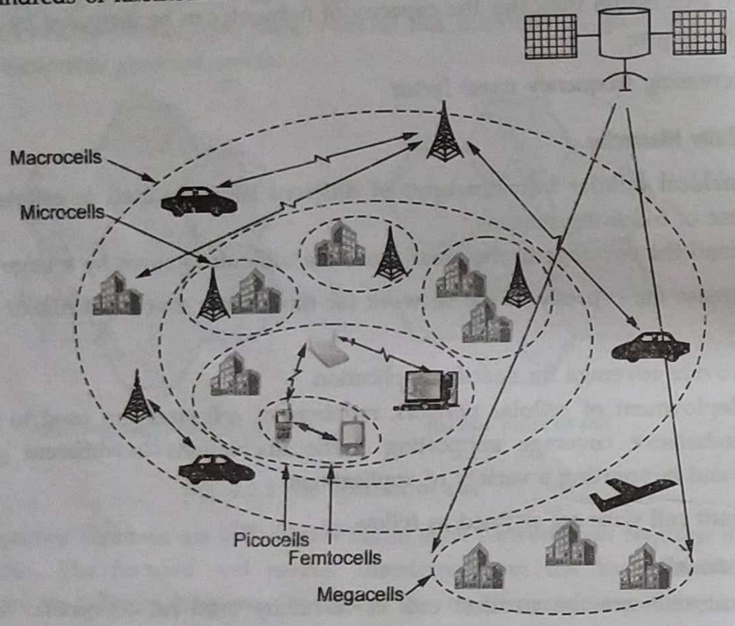


Fig. 2.1.3 Coverage areas of different cells

Solved Example

Example 2.1.1 *A service provider wants to provide cellular communication to a particular geographic area. The total bandwidth the service provider licensed is 5 MHz and system subscriber requires 10 kHz of bandwidth. Determine the system capacity, if the service provider implements a cellular system with 35 transmitter sites and cluster size of 7.*

Solution : Given : Cluster size $N = 7$

$$\text{Total system bandwidth } B = 5 \text{ MHz} = 5000 \text{ kHz}$$

$$\text{Bandwidth per subscriber} = 10 \text{ kHz}$$

$$\text{Total cell transmitter} = 35$$

$$\text{Bandwidth per cell} = \frac{B}{N} = \frac{5000 \text{ kHz}}{7} \approx 714 \text{ kHz}$$

$$\text{Capacity of each cell} = \frac{714 \text{ kHz}}{10 \text{ kHz / user}} = 71 \text{ user}$$

$$\text{Total system capacity} = \text{Total number of cells * Capacity of each cell}$$

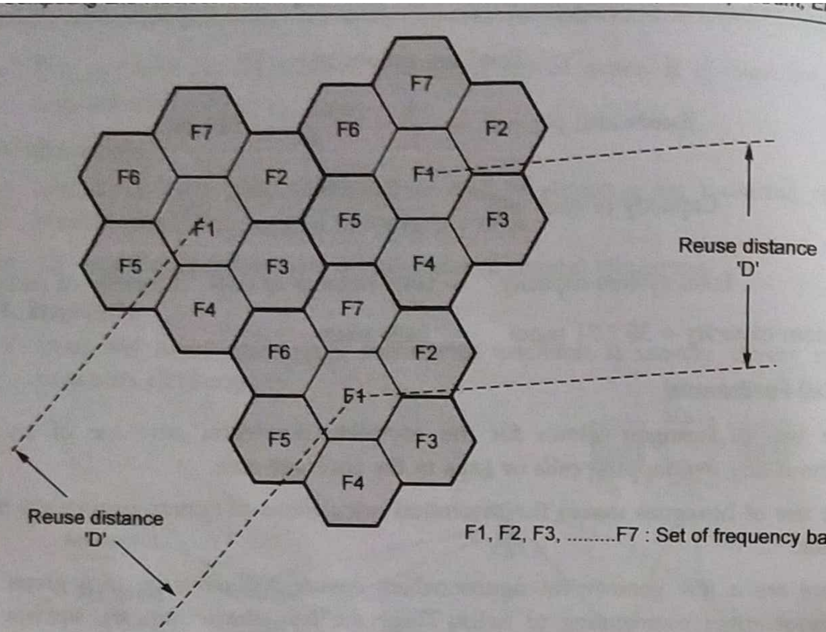
Total system capacity = 35 * 71 users = **2485 users**

2.1.1.4 Cell Fundamental

- The use of hexagon allows for the complete theoretical coverage of an area without any overlapping cells or gaps in the coverage area.
- The use of hexagons makes the theoretical calculations of system parameters much easier.
- There are a few geometrical figures which ensure full coverage of a given area without either overlapping or holes. These are equilateral triangles, squares and hexagons. Hexagons best approximate the circular shape of base station coverage in a flat terrain without obstacles and the hexagonal edges well approximate the borders between cells of the same size.
- In reality, the base station coverage does not have a regular circular shape because the coverage is a result of terrain architecture and obstacles such as houses, trees, etc.

2.1.2 Frequency Reuse

- In a cellular system, the frequency space allocated is insufficient. for a 7 cell cluster arrangement the allocation of frequencies into seven sets is required. The same frequency band or channel used in a cell can be reused in another cluster or cell i.e. frequency to be used for multiple simultaneous conversations. This is referred to as **frequency reuse.**
- Frequency reuse is the process of using the same set of frequencies to more than one cell. (See Fig. 2.1.4 on next page)
- However frequency reuse depends on various factors such as transmitter power of base station, antenna gain and height, distance between cells. The distance between the two cells using the same frequency is known as **reuse distance,** is denoted by D. A typical cluster of seven cells shows frequency reuse pattern and reuse distance.



F1, F2, F3, ...F7 : Set of frequency bands

Fig. 2.1.4 Frequency reuse for 7 cell cluster

- Frequency reuse distance is decided by cluster size 'N'. In hexagonal cell pattern the cluster size (number of cells per cluster) is given by,

$$N = i^2 + ij + j^2$$

where N represents the cluster size.

i represents the number of cells to be transversed along direction qi from center of cell.

j represents number of cells in direction 60° to the direction of i.

Substituting different values of i and j (nonnegative integers)

N = 1, 3, 4, 7, 9, 12, 13 ....

Most popular value of N are 4 and 7.

- Due to hexagonal geometry, there are six equidistant neighbours and each neighbor is separated by multiples of 60°.

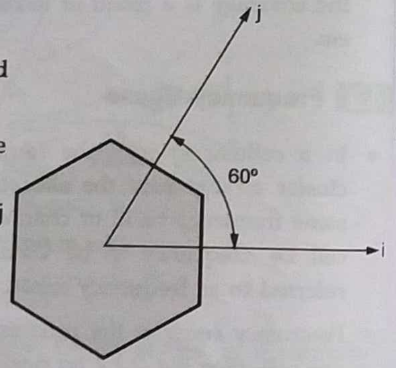


Fig. 2.1.5

2.1.2.1 Frequency Reuse Factor

- The relationship between frequency reuse distance 'D', radius and cell 'R' and number of cells per cluster 'N' is represented by,

$$\boxed{D = \sqrt{3N}\,R}$$

The ratio $\frac{D}{R}$ is known as **reuse factor.**

$$\frac{D}{R} = \sqrt{3N}$$

- Fig. 2.1.6 shows various reuse patterns.

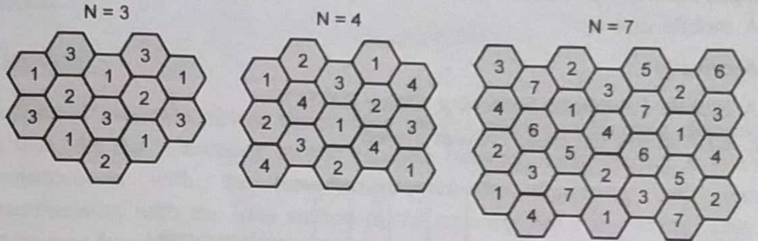


Fig. 2.1.6 Freuency reuse patterns for N = 3, N = 4 and N = 7

- If the system is not properly designed with respect to the number of cells in a cluster, topographic cell distribution and channel assignment, then it will experience excessive interference between the channels in different cells which use the same carrier frequencies.

Solved Examples

Example 2.1.2 *For a mobile system of cluster size of 7, determine the frequency reuse distance if the cell radius is 5 km. Repeat the calculation for a cluster size of 4.*

Solution : Given : Cluster size N = 7

Cell radius R = 5 km

Frequency reuse distance is given by $D = \sqrt{3N}R$

$D = \sqrt{3*7} * 5 = 4.5823*5$

$D =$ **22.913 km** ... Ans.

For cluster size $N = 4$

$D = \sqrt{3*4} *5 = 3.464*5$

$D =$ **17.32 km** ... Ans.

Example 2.1.3 *Determine frequency reuse distance for a cell radius of 2 km and cluster size of 8.*

Solution : Given : Cluster size N = 8

Cell radius R = 2 km

Frequency reuse distance is given by $D = \sqrt{3N}.R$

$$D = \sqrt{3*8} *2 = 4.8989*2$$

$$D = 9.7979 \text{ km}$$

2.1.3 Operation of Cellular System

- A basic cellular system consists of three parts :
  1. A mobile unit
  2. A cell site
  3. A Mobile Telephone Switching Office (MTSO)
- Fig. 2.1.7 shows the basic cellular system.

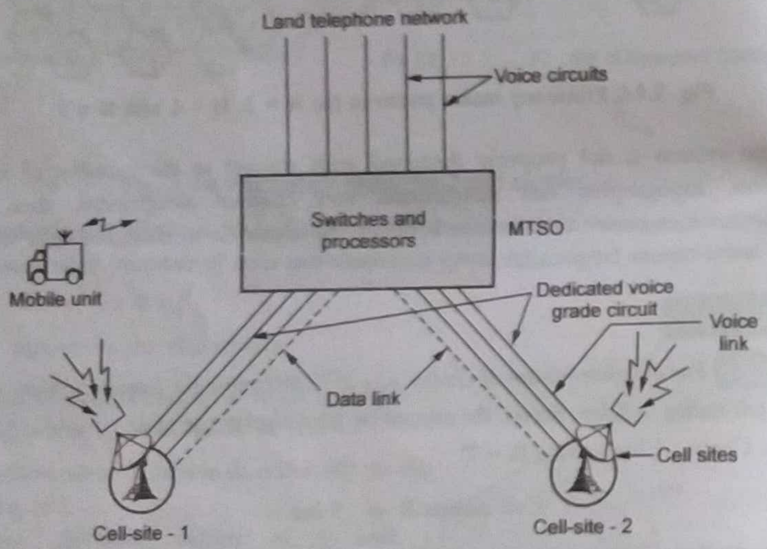


Fig. 2.1.7 Basic cellular system

1. **Mobile Unit :**
   - A mobile telephone unit contains a control unit a transreceiver and an anten system.
2. **Cell Site :**
   - The cell site provides interface between the MTSO and the mobile units. It ha control unit, radio, cabinets, antennas a power plant and data terminals.
   - Mobile unit is a transreceiver. It moves in any of the all sites.

3. **MTSO :**
   - The switching office and central co-ordinating element for all cell sites, contains the cellular processes and cellular switch. It interfaces with telephone company zone offices; controls call processing and handle billing activity.
   - MTSO provides coordination amongst the all sites and processor. It also performs the functions of overall administration. It also handles call processing and billing activities.

2.1.4 Handoff

- The limited available power transmitted by the mobile subscriber determined the cell size. As the subscriber moves (roams) between cells during a journey, the communication with the base station of the departing cell ceases and communication with the base station of the entering cell commences. This process is known as **handoff or handover.**
- Each adjacent base station transmits a frequency that is different from its neighbour. The handoff is accomplished when the received signal from the base station is low enough to exceed a predetermined threshold. At the border between two cells the subscriber is under the influence of two or even three base stations, and the communication link can pass back and forth between base stations as the moving subscriber receiver experiences a fluctuating field strength depending upon the immediate environment such as being surrounded by tall buildings. Hence the carrier-to-interference ratio (C/I) on its allocated channel will vary, this is monitored by main switching center,the mobile can be instructed to hand over the strongest base station.

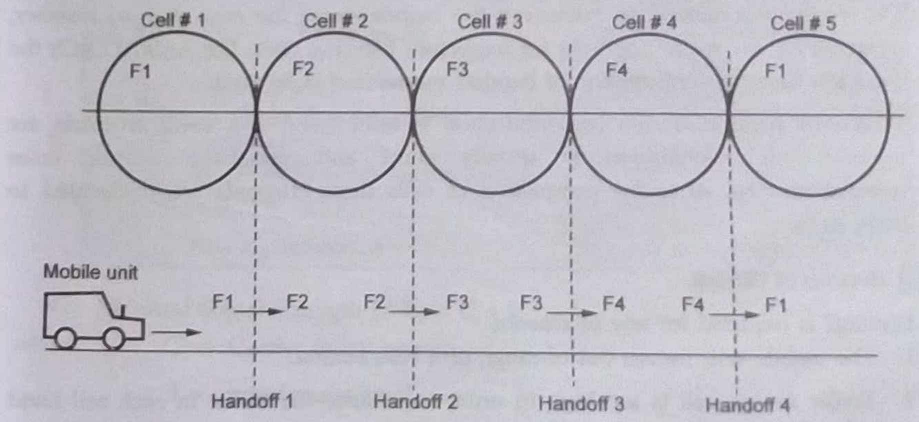


Fig. 2.1.8 Handoff mechanism

- Handoff mechanism is shown in Fig. 2.1.8 as the mobile unit passes throu adjacent cell sites maintained by local base stations.
- Handoff assures the continuity of calls. Handoff of a call to a new connecti implies transfer of security functions also.
- The handoff algorithm must be able to cope with-

  a) Whether the current loss in channel quality is due to short term fading.

  b) Whether a simple increase in power would be sufficient to restore the chan quality (it can produce an unacceptable co-channel interference in other c using the same frequency).

  c) Whether the measurements from adjacent cells are valid.

  d) Whether the cell chosen for handover has spare channels available.
- In some systems the mobile unit continuously monitors the signals of surround base stations and initiates the process of hand off when required. Such systems known as **mobile controlled handoff (MCHO).**
- In analogue systems such as in AMPS the base stations performs the radio chan measurments and the mobile terminal is totally passive it is known **network-controlled handoff (NCHO)**
- In digital systems, both mobile terminals and base stations make measureme and report these to fixed networks for handover decisions, it is known as mol **assisted handoff (MAHO).** It is used in GSM and IS 95.
- The handoff without interruption is called a **soft handoff,** it takes normally 0.2 to switch over. A handoff which that is broken momentarily during call transfe called **hard handoff.** During handoff, the information about the user stored in earlier base station is transferred to the new base station.
- On receipt a command to 'handover' the mobile stores the new channel numb power level and signalling tone for ms before handing over. For AMPS/TACS duration time for confirmation of handoff mechanism is 50 msec.
- Whenever handoff occurs communication is interrupted and voice channels muted. This interruption is usually short and unnoticed during vo communications. After the completion of calls these channels are reallocated other users.

2.1.4.1 Reasons of Handoff

- Handoff is required for any of reasons.
  1. The mobile unit moves out of range of a base station.
  2. Traffic in one cell is too high in order to balance the traffic in each cell ha off is initiated.

3. In noise limited system when the signal strength goes below the threshold of – 100 dBm.
4. When the signal strength is not at all reaching within the cell site. This happens because of geographical locations and the portion where the signal is not available is called as **holes or gaps.**
5. When the capacity for connecting new calls of a given cell is used up.
6. When there is interference in the channels due to the different phones using the same channel in different cells.

2.1.4.2 Types of Handoff

- Handoff is the mechanism which transfers an ongoing call from one cell to another cell as users are near to the coverage area of the neighbouring cell. If handoff does not occur quickly, the Quality of Service (QoS) will degarde below an acceptable level and the connection will be lost.
- There exists two types of handoff -

  1. Handoff based on signal strength.

  2. Handoff based on carrier-to-interference ratio (C/I).
- While designing the mobile system the minimum acceptable level of signal strength is decided. For noise-limited system the signal strength is –100 dBm and for interference limited system the threshold is – 95 dBm. When the signal level in any situation goes below the threshold level, the hand is initiated.
- Also for an acceptable quality of voice the value of carrier-to-interference ratio is decided within cell boundary. When the C/I ratio drops below 18 dB with cell area, handoff initiated.

Sr. No.	Based on SS	Based on C/I
1.	Threshold level i) – 100 dB M in noise limited systems ii) – 95 dB M in interference limited systems	At cell boundary C/I = 18 dB
2.	Easy implementation	Not easy to implenent

- Received Signal Strength (RSS) = C + I

where C → Carrier signal power

I → Interference level

- If C/I drops in a cell and if the occurance of handoffs is dependent on C/I then in this case as a response to drop C/I either the propagation distance or interference will increase.

2.1.4.3 Dropped Call

- When a mobile unit moves into a cell where all the channels are busy, there is possibility that the call may be dropped because of lack of free channels, it is called as **blocked call**. The reason of blocked call is non-availability of voice channels.
- The call may drop because of poor signal of the assigned voice channel the termination of call due to weak signal is referred to as **dropped call**. The signal becomes weak because of fading phenomena. The dropped call rate should be minimum to achieve the maximum efficiency of the system.

Dropped call rate is given by

$$p = \sum_{n=0}^{N} \alpha_n \cdot P_n$$

where P_n represents probability of dropped call after n handoff.

α_n represents weighted value for calls having n handoff.

N represents the maximum number of handoff.

2.1.4.4 Handoff Initiation

- In the cell site the signal strength is continously monitored using a reverse voice channel. Depending on the strength the decision for handoff is made.
- If the signal strength reaches a level that is higher than the threshold level set for minimum voice quality, cell site will request the switching office (MTSO) for handoff to continue the call. Occurance of handoff either earlier or later can be determined by intelligence within the call site also.
- Two points have to be considered and they should be avoided,
  1) An unneccessary handoff will be requested if the handoff decision is very early.
  2) A failure handoff would result if the handoff decision is very late.
- Thus the decision for a handoff on call should be perfect depending on accuracy of signal strength measurements. The threshold can be determined by two parameters namely velocity of vehicle 'V' and the pathloss slope γ in the pathloss curve.

- Assume the threshold level is – 100 dBm at cell boundary. To have a handoff here the signal strength level should be higher than – 100 dBm (Δ).
- If signal strength is = – 100 dBm + ΔdB then a request for handoff will be initiated. The value of Δ should not be too large or too small so that proper handoff initiation at right time will be made.

Note

Handoff may be necessary but cannot be done at following cases

1) Mobile is at signal strength hole and not at cell boundary.

2) If the mobile is at cell boundary but no channel in the new cell is available to make handoff

- In these cases MTSO has to take step to make handoff faster before a dropped call occurance.

Number of handoffs

- If the call size is smaller the number of handoffs taking place will be high.

The number of handoffs for one call progress depends on the size of the cell.

e.g.	Cell area	Number of handoffs
	16 to 24 km cell	0.2 handoff / call
	3.2 to 8 km cell	1 - 2 handoffs / call

2.1.4.5 Delaying Handoff

- In simple case of handoff we have an efficient call communication without disturbance inspite of the moving mobile unit's status.
- There is also another handoff called as two-handoff-level that is applied to have successive handoff of a call.
- The use of this algorithm allows two request handoffs so as to provide more chances to have a successful handoff.

2.1.4.6 Delayed Handoff

- When a base station wants to handover the call to the base station of new cell where the subscriber enters, the new base station will accept it and takes call control. This smooth handoff is possible only if the new cell is free to take it. If there the cell not available (free) then the handoff will be delayed. This is known as delayed handoff scenario.

- A simple two-level handoff technique is shown below with a graph mentioning threshold level.

There are two cases 1 and 2 as shown.

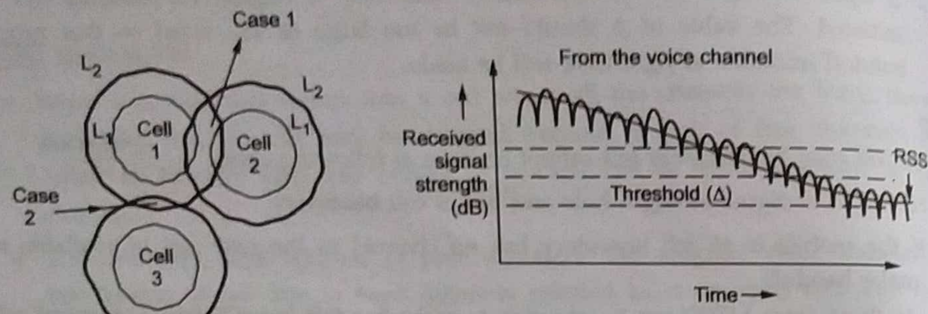


Fig. 2.1.9 Two level handoff technique

Assume that the mobile unit is in a hole or a weakspot or the neighbouring cell o it would be busy. Then handoff will be periodically requested say for every 5 sec.

- Consider the case 1. During first handoff level there will be successful handoff i the new signal is very strong. In case 2. the second handoff level is shown. Hen the call in progress is handed it to new cell with no restricted conditions.
- When there are both handoff request and originating call request comes present a same time to MTSO, the MTSO will attend to the handoff call first. The originating new call will be given second priority. The call will be allowed to continue smoothly till the allowed threshold level is reached, as in the graph Once the threshold level (Δ) is reached the call will be dropped.

Note If the SAT tone is not sent from mobile unit within a time of 5 sec, then cell site will turn off the transmitter unit. Thus receiving of SAT tone from mobile unit is closely monitored.

Advantages of delayed handoff

1) If the neighbouring cells are busy delayed handoff helps to continue the call in progress smoothly till the new cell gets free.
2) In two-handoff-level alogorithm only after the second handoff the call will be dropped. Thus probability of call blocking is very less.
3) This algorithm also makes handoff to take place at correct location.
4) The algorithm avoids interference in the system.

2.1.4.7 Forced Handoffs

- A forced handoff technique can be explained with two different definitions

1) Forced handoff is a technique that is defined as a handoff which should not occur but it is forced to occur.
2) Forced handoff is a technique that is defined as a handoff that would occur normally but it is prevented to occur.

- In forced handoff two important aspects are :
  i) Controlling a handoff and ii) Creating a handoff

I) Controlling a handoff

- If handoff should occur earlier then handoff threshold level should be high. On the otherhand if handoff should occur later the handoff threshold level should be low.
- Depending upon these criteria a cellsite has to plan a low handoff threshold or high handoff threshold level in the cellsite.
- The Mobile Switching Office (MSC) can also control the handoff and make it to occur either earlier or later, after receiving a handoff request from the cell site in the system.

II) Creating a handoff

- The concept of creating a handoff is dependent on the cell congestion due to mobile traffic.
- If a cell is too congested then mobile switching office decides to create handoffs.
- It informs the cellsite those that are heavily congested due to mobile traffic to create early handoffs. If so some calls will be handed over to neighbour cells and the congested cell will be reaching a moderate mobile traffic.
- Thus handoff threshold level in cell site may be high or low according to the order of MTSO given to cellsites. Depending upon the instructions of MTSO either earlier or delayed handoff would take place in the cell.

The advantage of this method is to have an efficient mobility management.

2.1.5 Power Control

- Dynamic power control is necessary in a cellular system for the following reasons :
  1. The received power must be sufficiently above the background noise for effective communication, which states the required transmitted power.
- As the mobile unit moves away from the transmitter, the received power rejects due to normal attenuation.

- Also, the effects of reflection, diffraction and scattering can cause rapid changes in received power levels over small distances.
- This is because the power level is the sum from signals coming from a number of different paths and the phases of those paths are random, sometimes adding and sometimes subtracting.
- As the mobile unit moves, the contributions along various paths change

2. It is desirable to minimize the power in the transmitted signal from the mobile unit, to reduce co-channel interference (interference with channels on the same frequency in remote cells), alleviate health concerns, and save battery power.
3. In Spread Spectrum (SS) systems using Code Division Multiple Access (CDMA), it is desirable to equalize the received power level from all mobile units at the BS.

- This is crucial to system performance because all users have the same frequency allocation.

2.2 First Generation Analog System

- The first analog, voice oriented cellular telephone system launched during 1970s and 1980s is referred to as first generation or 1G cellular technology.
- The first generation cellular system used analog frequency modulation schemes for transmission with two isolated bands downlink (from base station to mobile) and uplink (from mobile to base station) transmission. It uses Frequency Division Multiplexing (FDM) to increase system capacity.
- Different 1G cellular technologies are :
  1. Advanced Mobile Phone System (AMPS)
  2. Total Access Communication System (TACS)
  3. Nordic Mobile Telephone (NMT - 450)
  4. Nippon Telegraph and Telephone (NTT)
  5. Japanese TACS (JTACS)
- Table 2.2.1 summarizes different 1G analog cellular systems.

Standard	Forward band (MHz)	Reverse Band (MHz)	Channel spacing (kHz)	Region	Comments
AMPS	824 - 849	869 - 894	30	United States	Also in Australia, Southeast Asia, Africa
TACS	890 - 915	935 - 960	25	EU	Later, bands were allocated to GSM
E-TACS	872 - 905	917 - 950	25	UK	
NMT 450	453 - 457.5	463 - 467.5	25	EU	
NMT 900	890 - 915	935 - 960	12.5	EU	Freq. overlapping; also in Africa and southeast Asia
C-450	450 - 455.74	460 - 465.74	10	Germany, Portugal	
RMTS	450 - 455	460 - 465	25	Italy	
Radiocom 2000	192.5 - 199.5	200.5 - 207.5	12.5	France	
	215.5 - 233.5	207.5 - 215.5			
	165.2 - 168.4	169.8 - 173			
	414.8 - 418	424.8 - 428			
NTT	925 - 940	870 - 885	25/6.25	Japan	First band is nationwide, others regional
	915 - 918.5	860 - 863.5	6.25		
	922 - 925	867 - 870	6.25		
JTACS/NTACS	915 - 925	860 - 870	25/12.5	Japan	All are regional
	898 - 901	843 - 846	25/12.5		
	918.5 - 922	863.5 - 867	12.5		

Table 2.2.1 Existing 1G analog cellular systems

2.2.1 AMPS

- Due to increasing demand of mobile users, the available channels are not enough to accomodate new users. The solution can not be simply to assign new frequencies as the spectrum space for new approach to mobile telephony was needed. Hence a system called Advanced Mobile Telephone System (AMPS) was deployed in 1983 in Chicago.
- AMPS uses cellular concept based on many repeaters. The cellular radio technology was more efficient and can provide high quality mobile service to maximum subscribers.

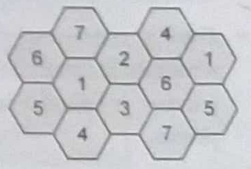


Fig. 2.2.1 Cell structure

- A total 40 MHz of spectrum bandwidth is 800 MHz band was allocated to AMPS. The AMPS uses seven cells reuse pattern with provisions for sectoring and cell splitting to increase capacity. There are many repeaters responsible for coverage in a cell. The cell shapes are hexagonal ideally as shown in Fig. 2.2.1.

- All the cell sites are interconnected by fiber optics or microwave link to Mobile Telephone Switching Office (MTSO) or Mobile Switching Center (MSC). All the calls are routed through cell center and MTSO. No mobile users are directly connected.
- Each cell site transmitter operates at comparatively low power frequency reuse is possible after some distance. The available bandwidth is divided amongs the cells.

2.2.2 Cellular Carriers and Frequencies

- Each carrier has 395 duplex voice channels and 21 control channels to setup calls and administer housekeeping activities like registration and paging. For voice modulation narrowband analog FM is used with maximum frequency deviation of 12 kHz and channel spacing of 30 kHz.
- Two carriers are used known as A and B carrier. A represents non-wireline carrier and B is for wire line carrier. Each carriers are assigned 832 frequencies (790 voice and 42 data). A pair of frequency is used to create one channel. Transmission from base to mobile is called as **forward channel** and transmission from mobile to base is called as **reverse channel**.
- In North American system, reverse channel transmission uses frequency in range of 824 MHz to 849 MHz and forward channel transmission uses frequency in the range of 869 MHz to 894 MHz.

2.2.3 Channel Allocation

- The control channels are used to allocate voice channels to the user. After dialling a telephone number and then pressing send button, the phone scans all the control channel frequencies for a strongest signal. The cell phone transmits its corresponding control channel and once the call is established the cell sites assigns it a clear voice channel.
- During conversation, the adjacent cell monitors the signal strength, when signal strength is greater in an adjacent cell, the call is transferred to that cell. This process is called **handoff**. Thus handoff requires a change in frequency for mobile phone.

2.2.4 AMPS Operation for Mobile Originated Calls

- It is a mobile to land call. If a mobile subscriber wants to make a call, there is exchange of several messages over the control channels such as :

1. Handshaking operations
2. Signaling operations
3. Service requests

- Fig. 2.2.2 shows steps involved in mobile originated calls.

Step 1 : Mobile seizes to reverse control channel (RECC).

Step 2 : Once mobile seizes the RECC, it starts transmitting service request message to base station over RECC.

Step 3 : On granting the service request it sends initial voice channel designation message.

Step 4 : Base and mobile stations switched their communication to the voice channel specified.

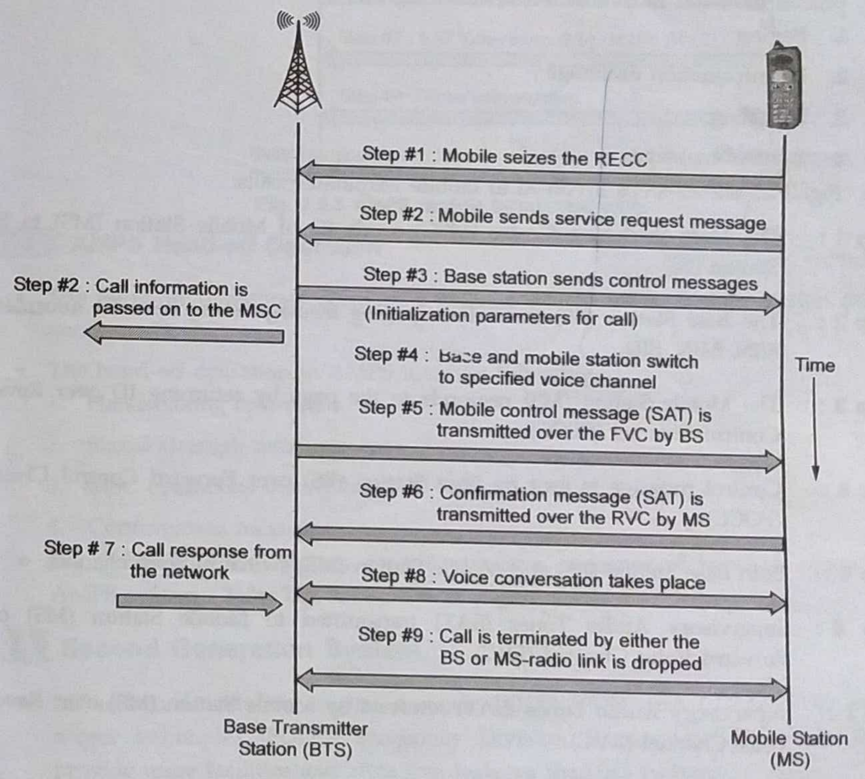

Step #1 : Mobile seizes the RECC
Step #2 : Mobile sends service request message
Step #3 : Base station sends control messages
(Initialization parameters for call)
Step #2 : Call information is passed on to the MSC
Step #4 : Base and mobile station switch to specified voice channel
Time
Step #5 : Mobile control message (SAT) is transmitted over the FVC by BS
Step #6 : Confirmation message (SAT) is transmitted over the RVC by MS
Step # 7 : Call response from the network
Step #8 : Voice conversation takes place
Step #9 : Call is terminated by either the BS or MS-radio link is dropped
Base Transmitter Station (BTS)
Mobile Station (MS)

Fig. 2.2.2 AMPS mobile originated calls

Step 5 : The base station sends a mobile control message over Forward Voice Chann (FVC) with Supervisory Audio Tones (SAT).

Step 6 : Mobile station sends transmits confirmation message (SAT) over Reverse Voi Channel (RVC).

Step 7 : Mobile station awaits completion of call with response from network.

Step 8 : Voice conversation takes place.

Step 9 : Either base station sends a release order message or mobile sends a signalli tone at which point the BS and MS drop the voice channel radio link.

2.2.5 AMPS Operation for Mobile Terminated Calls

- The mobile terminated calls are land-to-mobile and mobile-to-mobile calls. Vario phases involved in mobile terminated calls are
  1. Paging
  2. ID information exchange
  3. Signaling
  4. Control messages
- Fig. 2.2.3 shows steps involved in mobile terminated calls.

Step 1 : The Main Switching Centre (MSC) sends ID of Mobile Station (MS) to B Station (BS).

Step 2 : The Base Station (BS) transmits a paging message along with ID informati ESN, MIN, SID.

Step 3 : The Mobile Station (MS) responds to the page by returning ID over Reve Control Channel (RECC).

Step 4 : Control message is sent by Base Station (BS) over Forward Control Chan (FOCC).

Step 5 : Both Base Station (BS) and Mobile Station (MS) switch to voice channel.

Step 6 : Supervisory Audio Tones (SAT) transmitted to Mobile Station (MS) o Forward Voice Channel (FVC).

Step 7 : Supervisory Audio Tones (SAT) returned by Mobile Station (MS) over Reve Voice Channel (RVC).

Step 8 : After last handshake signal, the traffic channel is opened to conversati between Base Station (BS) and Mobile Station (MS).

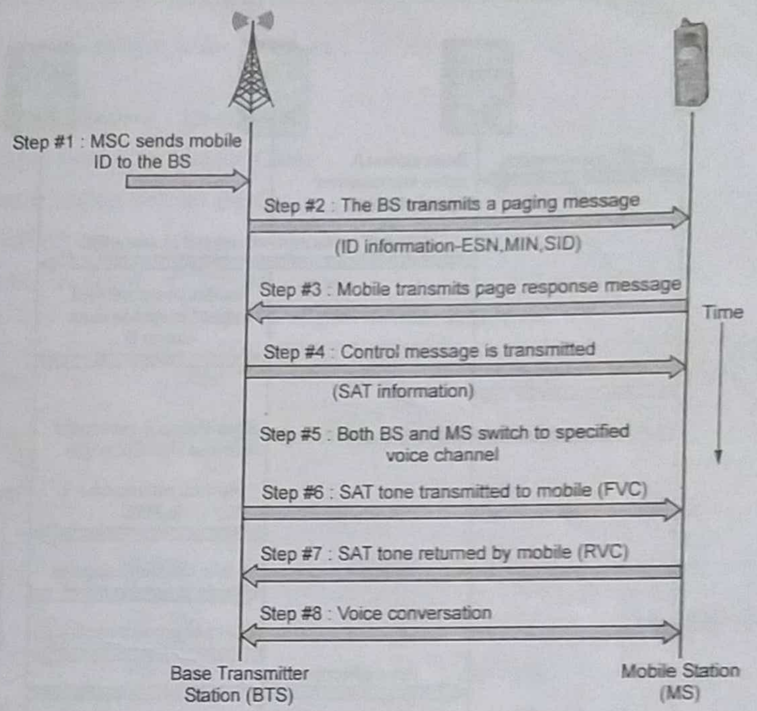

Step #1 : MSC sends mobile ID to the BS
Step #2 : The BS transmits a paging message
(ID information-ESN,MIN,SID)
Step #3 : Mobile transmits page response message
Time
Step #4 : Control message is transmitted
(SAT information)
Step #5 : Both BS and MS switch to specified voice channel
Step #6 : SAT tone transmitted to mobile (FVC)
Step #7 : SAT tone returned by mobile (RVC)
Step #8 : Voice conversation
Base Transmitter Station (BTS)
Mobile Station (MS)

Fig. 2.2.3 AMPS mobile terminated calls

2.2.6 AMPS Hand-off Operation

- The hand-off operations occur in a cellular system when Mobile Station (MS) to another cell.
- The hand-off operation in AMPS involves following :
  1. Handshaking operations
  2. Signal strength measurements
  3. MSC operations during hand-off
  4. Confirmation messages.
- Fig. 2.2.4 illustrates various control messages sequence of hand-off operation in AMPS system. (Refer Fig. 2.2.4 on next page)

2.3 Second Generation System

- 2G standards rely on digital formats TDMA/FDD and CDMA/FDD multiple access techniques (FDD - Frequency Division Duplexing). 2G cellular systems provide more facilities and attractive features than 1G systems.

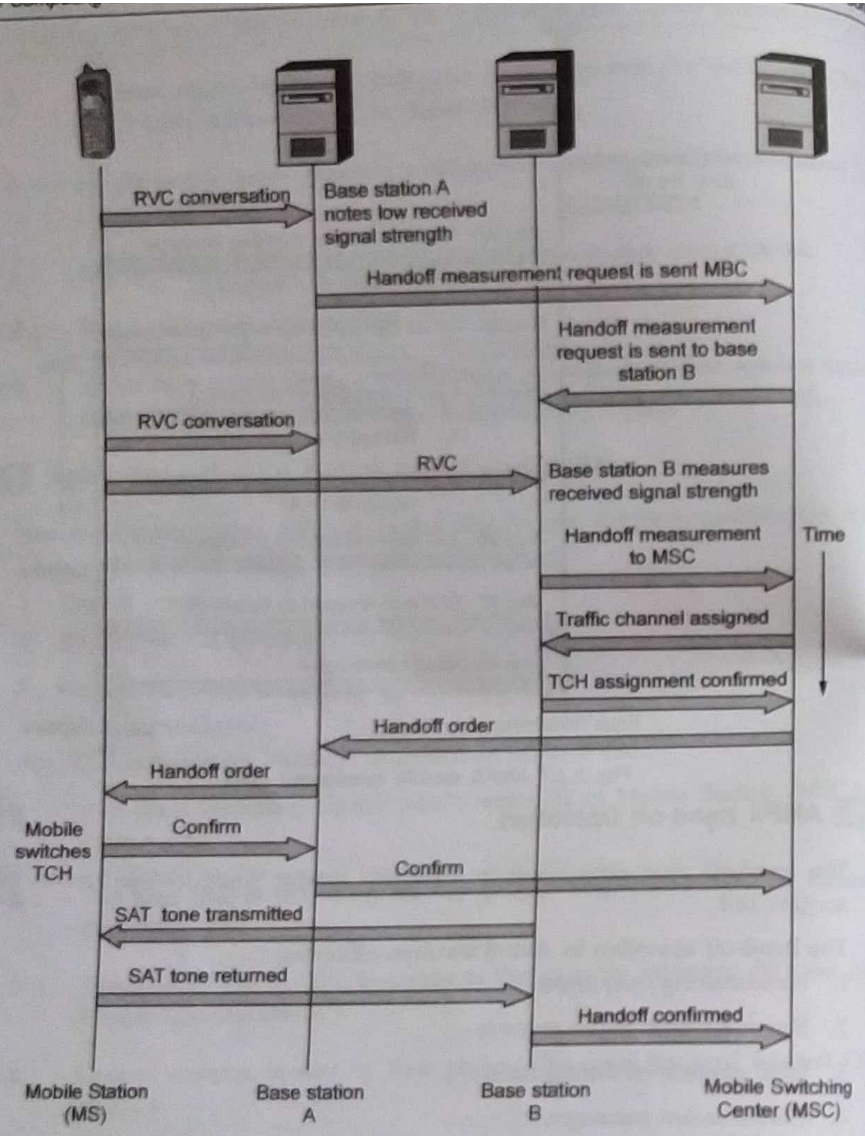


Fig. 2.2.4 Hand-off operation in AMPS

- Features of 2G cellular systems are :
  1. Better speech quality.
  2. High speed data application.
  3. Efficient spectrum utilization.
  4. Supports multiple users.

- Different 2G cellular technologies are :

  A] TDMA :

  1. Interim Standard - 136 (IS - 136)
  2. Global System for Mobile (GSM)
  3. Pacific Digital Cellular (PDC).

  B] CDMA :

  1. Interim Standard - 95 (CDMA - one)

- Table 2.3.1 summarizes major 2G digital cellular standards.

System	GSM	IS-54	JOC	IS-95
Region	Europe / Asia	United States	Japan	United States/Asia
Access method	TDMA/FDD	TDMA/FDD	TDMA/FDD	CDMA/FDD
Modulation scheme	GMSK	π/4 - DQPSK	π/4 - DQPSK	SQPSK/QPSK
Frequency band (MHz)	935 - 960 890 - 915	869 - 894 824 - 849	810 - 826 940 - 956 1,477 - 1,489 1,429 - 1,441 1,501 - 1,513 1,453 - 1,465	869 - 894 824 - 849
Carrier spacing (kHz)	200	30	25	1,250
Bearer channels/carrier	8	3	3	Variable
Channel bit rate (kbps)	270.833	48.6	42	1,228.8
Speech coding	13 kbps	8 kbps	8 kbps	1 - 8 kbps (variable)
Frame-duration (ms)	4.615	40	20	20

Table 2.3.1 2G digital cellular standards

2.3.1 Second Generation TDMA

- In TDMA system, a number of users share the same frequency band by ta assigned turns in using the channel.
- A base station controller assigns time slots to users and slot released upon completion of call.
- The entire band is used by the user during his slot. Fixed assignment em predetermined order. Slot is wasted if there is no information for transmission

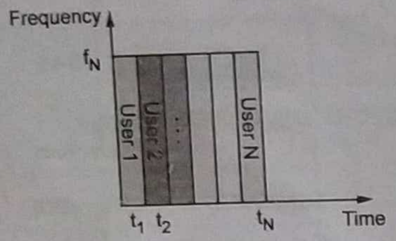


Fig. 2.3.1 TDMA

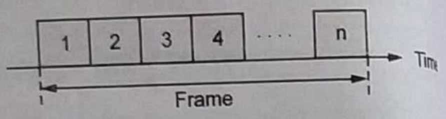


Fig. 2.3.2 TDMA frame structure

2.3.1.1 Advantages of TDMA

1. At a given time only one carrier is present on the channel hence intermodu distortion is eliminated.
2. TDMA transmission is separated in time domain. Processing of signal in domain is easier.
3. TDMA is most efficient method of transmission because of efficient u transmission resources.
4. TDMA can accomodate a wider range of bit rates by allowing a station allocated several slots. Thus TDMA is more flexible than FDMA.
5. No intermodulation products (if the full transponder is occupied).
6. Saturated transponder operation possible.
7. With a flexible Burst Time Plan it will optimize capacity per connection.

2.3.1.2 Disadvantages of TDMA

1. Precise synchronization between stations is required. Transmission of every sl must occur during exact time slot.
2. Bit and frame timings must be maintained by TDMA.
3. Requires network-wide timing synchronization.
4. Analog signals must be converted to digital.
5. Interface with analog terrestrial plants is expensive.

2.3.1.3 Advantages of TDMA over FDMA

1. Digital equipment used in time division multiplexing is increasingly becoming cheaper.
2. There are advantages in digital transmission techniques. Example : Error correction.
3. Lack of inter-modulation noise means increased efficiency

2.3.2 Second Generation CDMA (IS-95)

- IS-95 system uses Code-Division Multiple Access (CDMA) by means of Direct Sequence Spread-Spectrum modulation (DS-SS).
- Code Division Multiple Access (CDMA) is one of the basis for many of the commercial 2 G cellular systems around the world and is also used in many other types of communications systems, including Personal Communication System (PCSs), fixed wireless (wireless local loop), Global Positioning System (GPS) and the OmniTRACS satellite system for transportation logistics. CDMA is also known as IS-95, which refers to original ITU IS-95 wireless Interface protocols.
- CDMA system users are distinguished from each other by a code rather than by alloted time slot as in GSM. A single physical link (channel) is 1.23 MHz wide and typically 12 subscribers share the same link simultaneously. An important feature of CDMA is that neighbouring cells or sectors in cells can use the same physical channel.

2.3.2.1 Principles of CDMA

- CDMA systems allow many data signals to be multiplexed and transmitted over a wireless channel at the same time and in same frequency band without interfering with each other. It is done by deliberately spreading the spectrum occupied by user with high speed codeword unique to that user. The spectrum spreading is done by multiplying the user data by identifying code and modulating a carrier with resultant waveform (spread spectrum). At the receiver original data is recovered by correlating the demodulated waveform by original spreading code.
- The spread spectrum technique used in CDMA is of direct sequence type. The data signals to be transmitted are modified through the use of pseudo-noise code (PN code). In time division systems, channels are separated by time slot they occupy but in code division systems, channels are distinguished according to which PN code they use.
- The PN codes used in a system are orthogonal means the codes should not correlate among themselves nor they be time shifted version of each other. Therefore, each signal with a unique PN code can be detected from other signals.

When a PN code is auto-correlated, the result is high (1) but when cross-corre with other PN code in the same set, the result is zero (0). PN coded sequenc generated by using one or more shift registers with specific feedback connect This PN spreading code is often called as *chipping code*. An important characte of spread spectrum system is its processing gain G_P, which is proportional t ratio of spreading code rate to the data rate.

$$G_P = \frac{R_{chip}}{R_{data}}$$

PN codes used in CDMA

- CDMA system uses three types of PN code.
  1. Walsh code
  2. Long PN code
  3. Short PN code

1. Walsh code : CDMA use of walsh code is of 64 different orthogonal codes used

a. Downlink - For different user (spreading). It is a code channel.

b. Uplink - Not to differentiate users but for modulation.

2. Long PN code : 42-bit code

a. Down link - Used for data scrambling.

b. Uplink - For identifying mobile station (spreading).

3. Short PN code : 16-bit code

a. Down link - Used to identify base stations.

b. Uplink - Mobile uses this code for extra signal robustness without offset.

Features of CDMA

1. Transmit rate of one channel	: 192 kbps
2. Number of time slots in one CDMA channel	: 64
3. Average data rate for each user	: 3 kbps
4. Two voice coding schemes	: 8 kB/s, 13 kB/s
5. Vocoder rate	: 1.25 Mbits/s
6. Power updates of mobile user	: Every 1.25 ms
7. Voice and data communication	: 1.25 MHz radio carrier

2.3.2.2 CDMA Architecture

- CDMA architecture is shown in Fig. 2.3.3.
- CDMA interfaces are as follows.
  1. A+ or A - bis : Interface between BSC and BTS (proprietary interface depends on vendor).
  2. IS + 634 : An open interface between MSC and BSC
  3. ANSI - 41 : An interface with other PLMNs.
  4. ISUP (ISDN user part) : Interface with user part.
  5. IS - 95 : This is an air interface between base station substation and mobile.

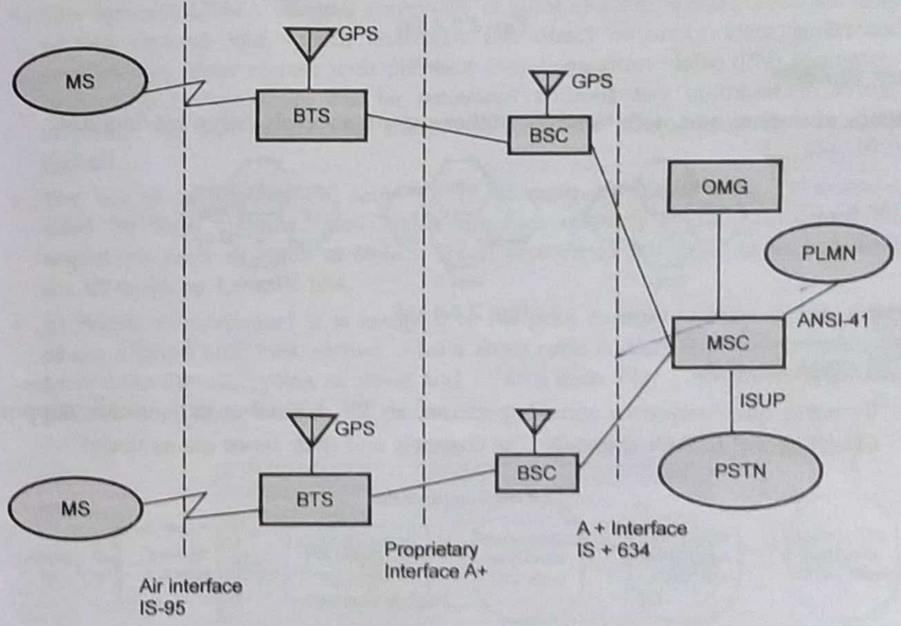


Fig. 2.3.3 CDMA architecture

2.3.2.3 CDMA Frequency Use

- With CDMA all the frequency band can be used in all cells. In CDMA, an RF channel uses carrier of 1.2288 Mb/sec with QPSK modulation. The bandwidth of a channel is 1.25 MHz. Because of this system capacity is increased many fold.
- Spread spectrum technique used frequency diversity this is very useful in mobile environment with multipath fading. CDMA system uses full 1.25 MHz BW for voice transmission.

- Since the frequency is not changing when mobile is crossing the cell, handoff i not required. Instead, CDMA system uses **soft handoff**. In soft handoff, mobi communicates with two cells simultaneously instead of switching from one cell t other. This gives space diversity of antennas. The comparison of hard handoff an soft handoff is shown in Fig. 2.3.4 (a) and (b).

A] Hard Handoff

Short blanking tones as mobile moves to cell.

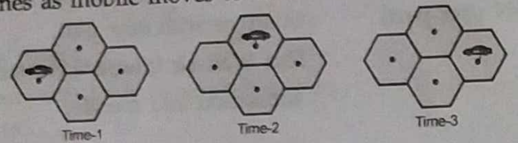


Fig. 2.3.4 (a)

B] Soft Handoff

Mobile communicates with two base stations simultaneously hence no data lost.

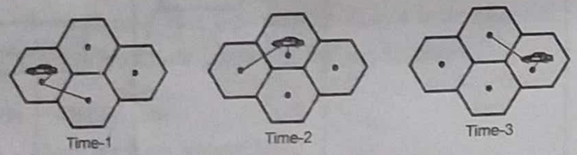


Fig. 2.3.4 (b)

2.3.2.4 CDMA Channels

- By using direct-sequence spread-spectrum, an RF channel at base station suppo 64 orthogonal CDMA channels. The channels and their types are as under -

CDMA channels		
55	–	Traffic channels
07	–	Paging channels
01	–	Synch channel
01	–	Pilot channel

- The total BW of CDMA is 1.25 MHz to be used for 55 voice channels. Therefo 22.7 kHz BW is allocated to each channel.
- Since all channels can be used in all sectors of all cells therefore CDMA is mo efficient in spectrum compared to any other system. In CDMA both forward an reverse channels are different.

2.3.2.5 Forward Channel / Downlink

- The downlink (forward channel) refers to transmission from the mobile station to base station. On the downlink, the PN codes are used as follows :

1. **Walsh codes** - To differentiate users (spreading),
2. **Short PN code** - To identify the cell (base station),
3. **Long PN code** - For data scrambling.

- Total downlink channels 64 for each carrier, out of which traffic channels are 55. The downlink traffic channels are used for information specific to MS during a call. It carries the control channels and user data (transmission and reception of speech, data and signalling). The basic user data rate is 9.6 kB/s and this is spread to a channel chip rate of 1.2288 Mchips/s using a combination of techniques.
- The forward CDMA channel comprises of pilot channel, synchronization channel, paging channel and speech channels. The direct sequence form is created by multiplexing these signals with different Pseudo-random Noise (PN) sequence. The orthogonal PN sequence can be recovered without any interference. When PN sequence are not orthogonal, there will be some mutual interference between signals.
- The use of orthogonal PN sequence is desirable. A Walsh code PN-sequence is used by base stations. The Walsh function consists of 64 orthogonal binary sequences, each of length of 64-bits. It can provide 64 independent logical channels for all users on forward link.
- In Walsh code, channel '0' is assigned to the pilot channel to keep mobile receivers phase aligned with base station. Also a short code is used for synchronizing and a long code for encryption of voice and control data. Fig. 2.3.5 shows spreading in CDMA voice channel.

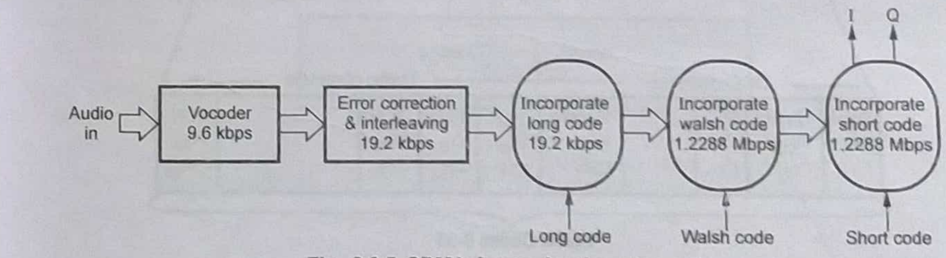

Audio in
Vocoder 9.6 kbps
Error correction & interleaving 19.2 kbps
Incorporate long code 19.2 kbps
Incorporate walsh code 1.2288 Mbps
Incorporate short code 1.2288 Mbps
I
Q
Long code
Walsh code
Short code

Fig. 2.3.5 CDMA forward voice channel

- The processing gain G_P, is given by -

$$G_P = \frac{B_{RF}}{B_{BB}} = \frac{\text{RF bandwidth}}{\text{Baseband bandwidth}}$$

$$G_P = \frac{1.2288 \times 10^6}{19.2 \times 10^3} = 64 = 18.06 \text{ dB}$$

Total spreading gain

$$G_P = \frac{1.2288\times10^6}{89.6\times10^3} = 128 = 21.1 \text{ dB}$$

- Such 64 orthogonal channels are transmitted on one RF carrier then QPSK modulator is used to modulate or single carrier. Fig. 2.3.6 shows multiplexing of CDMA channels.

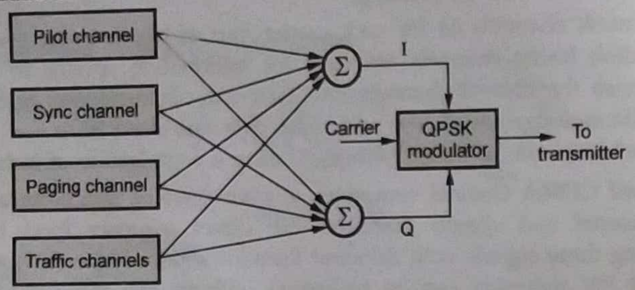


Fig. 2.3.6 Multiplexing CDMA channels

- The structure of downlink/forward channel is shown in Fig. 2.3.7.

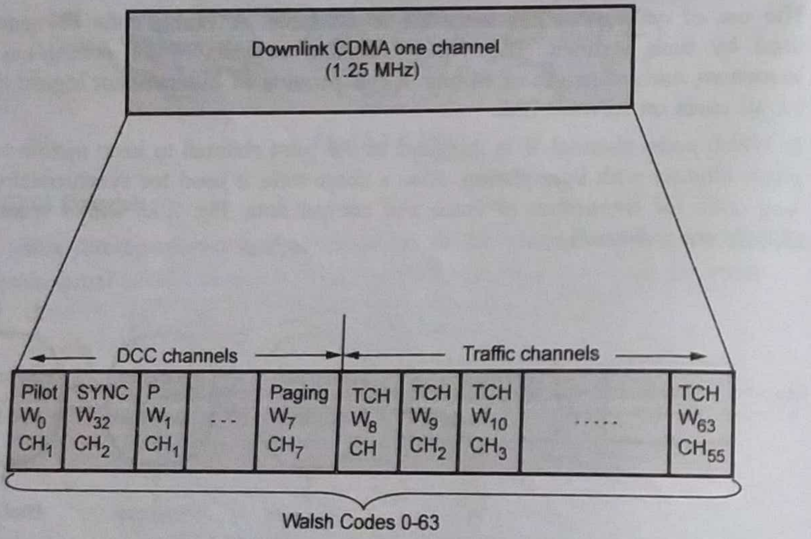


Fig. 2.3.7 Downlink structure

2.3.2.6 Reverse Channel / Uplink

- The uplink refers to transmission from base station to mobile station. The uplink frequency is built and arranged differently from downlink frequency. (45 MHz below forward channel frequency). The uplink (reverse channels) are coded with 1/3 rate convolutional PN long code. The unique MS equipment identifier is part of this PN code.

- On reverse channel, the PN codes are used as follows :
  1. Walsh codes are used for modulation (not to differentiate users).
  2. Short PN code is used by mobile for extra signal robustness without offset.
  3. Long PN code on uplink is used to identify the mobile station (spreading).
- There are only two types of channels on reverse link, traffic channels and access channels. The access channels are almost identical to traffic channels. The data access channel occurs at a fixed rate of 4800 b/sec in 20 ms frames and contains information required by the network to properly log the mobile terminal into service.

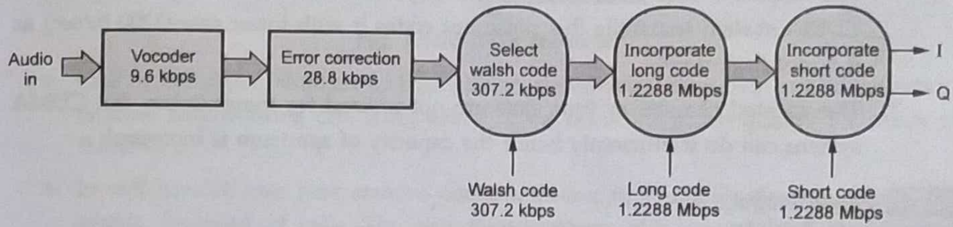

Audio in
Vocoder 9.6 kbps
Error correction 28.8 kbps
Select walsh code 307.2 kbps
Incorporate long code 1.2288 Mbps
Incorporate short code 1.2288 Mbps
I
Q
Walsh code 307.2 kbps
Long code 1.2288 Mbps
Short code 1.2288 Mbps

Fig. 2.3.8 CDMA reverse channel

- A truly orthogonal channels cannot be used by mobile units, as there is no pilot channel (phase coherent). Assigning individual pilot channel to each mobile will require much larger bandwidth. Therefore error correction code used is more robust type. Fig. 2.3.8 shows CDMA reverse voice channel.
- In reverse CDMA channel each code have different purposes. Long code is for distinguishing mobile, Walsh code is far decoding messages in presence of interference. The mobile unit uses offset QPSK modulation technique.
- The uplink structure is shown in Fig. 2.3.9.

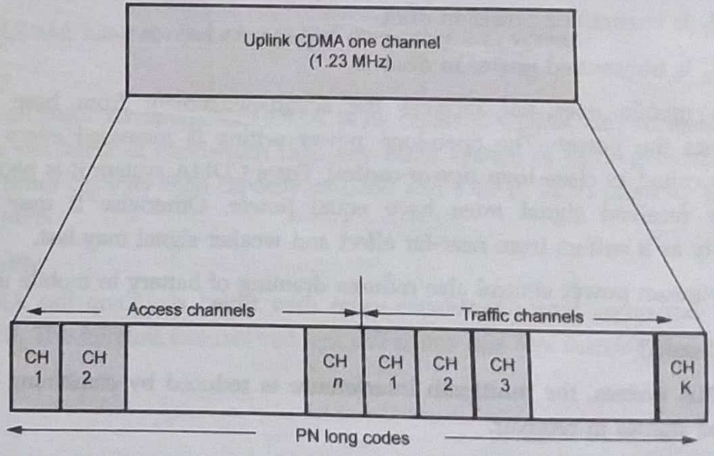


Fig. 2.3.9 Uplink structure

2.3.2.7 Voice Coding

- Variable rate vocoder is used for CDMA with 4 different bit rates i.e. 9600 bps, 4800 bps, 2400 bps and 1200 bps. When user is talking bit rate of 9600 bps is used and bit rate is reduced to 1200 bps during pauses.
- During a conversation, user actually talks for more than 50 %, during the pause the bandwidth allocated can be reassigned to other conversation.
- In FDMA or TDMA systems there exists two problems :
  1. When someone stops talking, the user assumes that the phone is disconnected. The reason is that there is always background noise even in quiet room. But CDMA system transmits this noise but codes it with lower rate (1200 b/sec) as it is not important.
  2. The vacated channel or time slots are not utilized for transmission. But CDMA system can do it efficiently hence the capacity of spectrum is increased.

2.3.2.8 Power Control

- Power control of mobile stations is important in CDMA systems.
- The power received at base station from mobile units must be within 1 dB.
- As mobile turns on it first measures power received from base station and then sets transmitter power assuming equal losses on reverse channel. This is known as open-loop power setting.
- The transmitted and received power are

$$\boxed{P_T = -76 \text{ dB} - P_R}$$

where, P_T is transmitted power in dBm

P_R is transmitted power in dBm

- If the mobile does not receives the acknowledgement from base station, it increases the power. The open-loop power setting is increased every 1.25 msec. This is called as **close-loop power control**. For a CDMA system it is necessary that all the received signal must have equal power. Otherwise it may not work properly as it suffers from near-far effect and weaker signal may last.
- The optimum power control also reduces draining of battery in mobile unit.

2.3.2.9 Soft Handoff

- In CDMA system, the multipath interference is reduced by combining direct and reflected signals in receiver.

- The signals received with different time delays are compensated for propagation times by a receiver called rake receiver shown in Fig. 2.3.10.

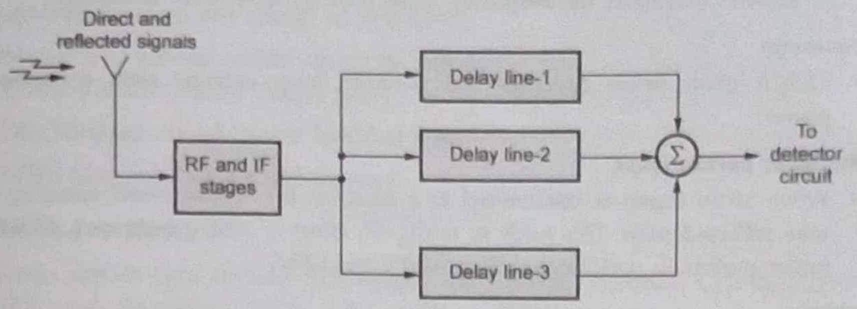


Fig. 2.3.10 Rake receiver

- One of the signal is taken as base station signal and other two can be reflections or from neighbouring cell. After every 20 ms decisions about quality are made on frame-to-frame basis.
- In soft handoff two base stations communicating to a mobile simultaneously, this avoids dropping of calls. The only disadvantage is increased load in switching station.

2.3.2.10 CDMA Security

- CDMA channel is not easily decodable. In order to decode a call it requires a spread spectrum receiver and despreading code also.
- The chances of eavesdropping are also small. It uses private key encryption. Therefore CDMA offers excellent security.

2.3.2.11 Advantages of CDMA

- The CDMA have several advantages over other 2 G systems.

1. Capacity

- One of major advantage of CDMA is its capacity. CDMA can accommodate more users per MHz of bandwidth than any other system of same generation. It has 4 to 5 times capacity than capacity of GSM and 8 to 10 times capacity than capacity of AMPS.

2. Call quality

- CDMA call quality is better with more consistent sound compared to GSM and AMPS. The handoff features reduces call drops and less interference.

3. **Frequency**

- CDMA uses one frequency per cell compared with maximum possible frequencies in TDMA. Therefore, the frequency reuse plan is much easier to manage.

4. **Coverage**

- CDMA gives better coverage and requires fewer antenna sites, consumes less power.

5. **Multipath performance**

- When radio signal is transmitted to a receiver, it can take direct route or it can take reflected path. This leads to multipath effect causing interference. CDMA has better multipath performance than AMPS and GSM.

2.3.2.12 Comparison of GSM and CDMA

Sr. No.	Parameters	GSM	CDMA
1.	Access mode	TDMA/FDD	CDMA/FDD
2.	Carrier (channel) spacing	200 kHz	1.25 MHz
3.	Time Slots (TS) in a frame-full-rate	8 TS	64 TS
4.	Time Slots (TS) in a frame-half-rate	16 TS	128 TS
5.	Downlink frequency (base station transmit to mobile subscriber)	925-960 MHz 1805-1880 MHz	869-894 MHz
6.	Uplink frequency (mobile subscriber transmit to base station)	880-915 MHz 1710-1785 MHz	824-849 MHz
7.	Frequency separation	45/95 MHz	45 MHz
8.	Carrier (channel) total bit rate	270.833 kbps	1228.8 kbps
9.	Full-rate coded traffic information (voice and data)-total sum of parameters : 10,11	22.8 kbps	About 77 kbps
10.	Error detection and correction bits	13 kbps	
11.	Full-rate, digitally coded speech	9.8 kbps	About 8/13 kbps
12.	Modulation technique	GMSK	QPSK/BPSK

2.3.3 2.5 Generation System

- 2.5G is an upgradation of existing 2G cellular system without any additional frequency spectrum and change in technology.
- Different 2.5G cellular system standards include :
  1. CDPD (Cellular Digital Packet Data)
  2. HSCSD (High Speed Circuit Switched Data)
  3. GPRS (General Packet Radio Service).

2.3.3.1 Mobile Data Services

- Various mobile data services technologies are : ARDIS, Mobitex, CDPD, TETRA, GPRS and Metricom. Table 2.3.2 compares different parameters of these technologies.

System	ARDIS	Mobitex	CDPD	TETRA	GPRS	Metricom
Frequency band (MHz)	800 bands 45 kHz sep.	935 - 940 896 - 961	869 - 894 824 - 849	380 - 383 390 - 393	890 - 915 935 - 960	902 - 928 ISM bands
Channel bit rate (kbps)	19.2	8.0	19.2	36	200	100
RF channel spacing	25 kHz	12.5 kHz	30 kHz	25 kHz	200 kHz	160 kHz
Channel access / Multiuser access	FDMA / DSMA	FDMA / Dynamic S-ALOHA	FDMA / DSMA	FDMA / DSMA	FDMA / TDMA / Reservn.	FHSS / BTMA
Modulation technique	4-FSK	GMSK	GMSK	π/4-QPSK	GMSK	GMSK

Table 2.3.2

2.4 Third Generation Systems

GTU : Winter-12

- 3G is a cellular system that supports higher data services, advanced multimedia services and global roaming. The 3G system ensures an efficient wireless access with high performance quality by using intelligent new protocols.
- Different 3G cellular system standards include :
  1. IMT 2000 and UMTS
  2. CDMA 2000.

2.4.1 UMTS/IMT 2000

- **Universal Mobile Telecommunications System (UMTS)** supports multi services, multiple QoSs, and higher data rates.
- The UMTS maximum packet-switched data rate is 1.960 Mbps, while t maximum circuit-switched rate is 384 kbps.
- Quality of Services (QoSs) parameters are set up when the channels are set up.
- QoSs can also be reconfigure without dropping the connection (circuit - packet-switched).
- The 3rd Generation Partnership Project (3GPP) is r ponsible for writing a maintaining the UMTS specifications.
- UMTS provides wireline voice quality, improved capa , and spectral efficienc
- UMTS uses AMR (adaptive multi-rate vocoder), an improvement over EFR GSM. Improved capacity is done with fast power control (1500 Hz vs. 2 Hz GSM) on both the UL and the DL.

2.4.1.1 Objectives of IMT 2000/UMTS

- The main objectives of IMT 2000/UMTS are -

1. Full coverage and mobility for rates up to 144 kb/s. Upto 2 Mb/s rates for mobility and limited coverage.
2. Use of different sized cells (macro, micro and pico) for indoor and out applications with seamless handover between them.
3. High spectrum efficiency compared to existing systems.

2.4.1.2 UMTS Architecture

- A UMTS system consists of three major subsystems :
  1. User Equipment (UE) 2. Access Network 3. Core Network
- Fig. 2.4.1 shows general architecture of UMTS.

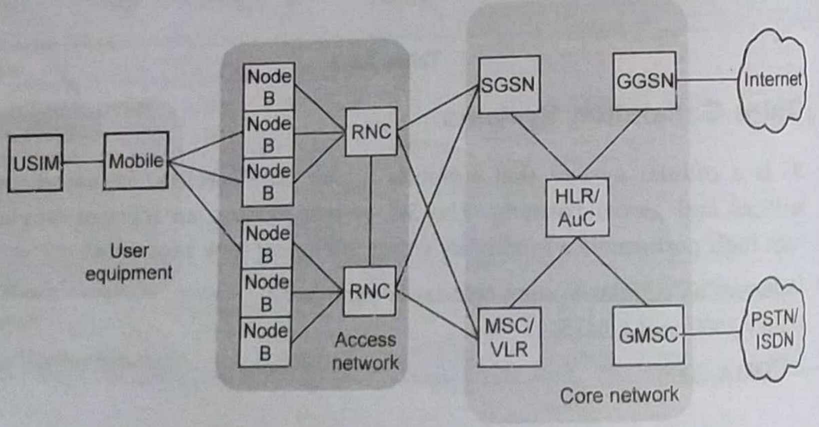


Fig. 2.4.1 UMTS architecture

1. **User Equipment (UE)**
   - UE can be a mobile, a fixed station, a data terminal, etc. It includes a USIM, which contains all of a user's subscription information.
2. **Access Network**
   - Access network includes all of the radio equipment necessary for accessing the network.
3. **Core Network**
   - Core network includes all of the switching and routing capability for connecting to either the PSTN (circuit-switched calls) or to a Packet Data Network (packet-switched calls), for mobility and subscriber location management and for authentication services.

Role of RNC

1. The RNC controls multiple node B_s through interface called I_{ub}. The associated RNC is known as **Controlling RNC (CRNC)** of the node B. The CRNC performs following functions.

   a) Load and congestion control of its own cells.

   b) Allocating new radio links to be established.
2. One UE connected to UTRAN (UMTS Terrestrial Radio Access Network) through only one Serving RNC (SRNC). The SRNC performs basic RRM (Radio Resource Management) operations such as handover decision and power control.
3. The RNC other than SRNC may be called as DRNC (Drift RNC). The DRNC controls cells used by the mobile. One User Equipment (UE) may have zero, one or more DRNCs.

2.4.1.3 UMTS Frequency Allocations

- Frequencies allocated in Europe for UMTS is shown in Fig. 2.4.2.

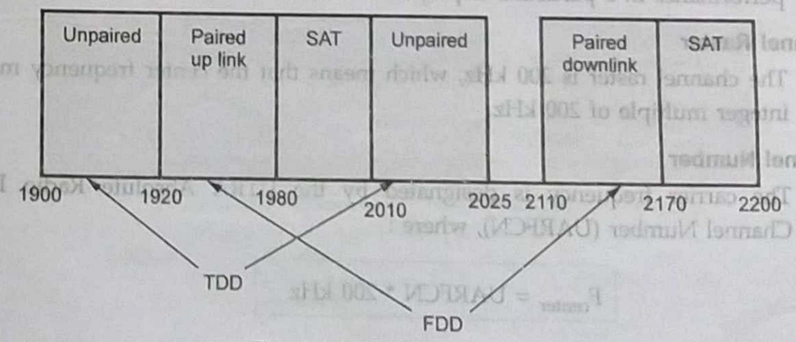


Fig. 2.4.2 UMTS frequencies

- UMTS FDD systems are currently specified to operate in the following pa bands :

Band	Uplink	Downlink
1	1920 to 1980 MHz	2110 to 2170 MHz
2	1850 to 1910 MHz	1930 to 1990 MHz

2.4.1.4 UMTS Bandwidth

- Fig. 2.4.3 illustrates bandwidth utilisation for UMTS.

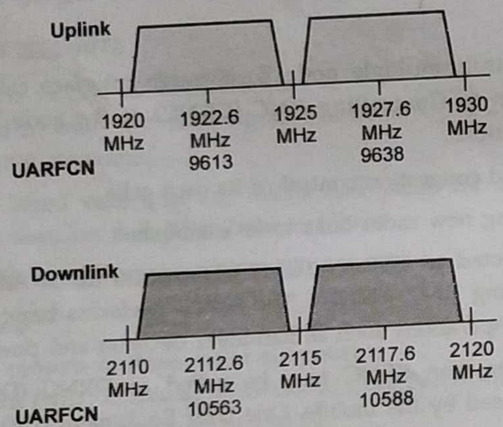


Fig. 2.4.3 UMTS bandwidth

Channel Spacing

- The nominal channel spacing is 5 MHz, but this can be adjusted to opti performance in a particular deployment scenario.

Channel Raster

- The channel raster is 200 kHz, which means that the center frequency must b integer multiple of 200 kHz.

Channel Number

- The carrier frequency is designated by the UTRA Absolute Radio Frequ Channel Number (UARFCN), where :

$$F_{center} = UARFCN * 200 \text{ kHz}$$

2.4.1.5 UMTS Air Interface

- The UMTS Terrestrial Radio Access (UTRA) interface was defined by the 3rd Generation Partnership Project (3GPP). It is often called WCDMA (Wideband CDMA) interface.
- WCDMA has two modes of operation differing in the kind of duplex transmission : FDD and TDD.
- In FDD mode, UMTS operates in paired bands, whereas in TDD mode UMTS operates in the unpaired bands. Both modes differ in their potential applications and details of their air interfaces.

2.4.1.6 UTRA FDD Mode

- In the UMTS FDD mode a physical channel is determined by the carrier frequency, the applied spreading sequence and the applied signal component (in the uplink, inphase and quadrature components can carry different physical channels).
- In the physical layer, two types of dedicated physical channels have been defined for uplink and downlink. They are :
  1. Dedicated Physical Control Channel (DPCCH)
  2. Dedicated Physical Data Channel (DPDCH).
- Physical channel is divided into 10-ms frames. The frames are further divided into 15 slots of 666.67 μs long.
- One dedicated physical control channel and up to six dedicated data channels are assigned to each connection.
- If the number of data channels (DPDCH) is higher than one, then the odd-numbered channels are summed, weighted and transmitted using the in-phase

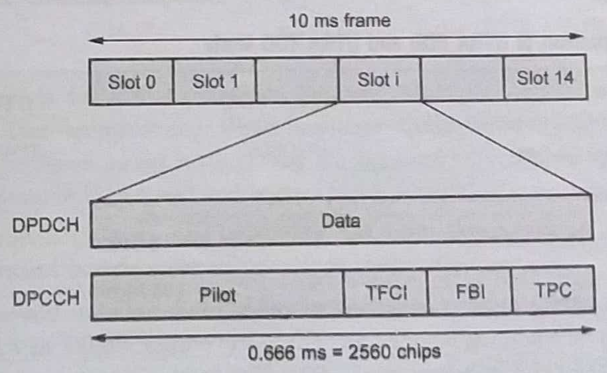


Fig. 2.4.4 Uplink dedicated physical channel structure

component, whereas the even-numbered channels are summed, weighted a transmitted together with the control channel (DPCCH), using the quadra component.

2.4.1.7 UTRA TDD

- In Time Division Duplex (TDD), time can be asymmetrically divided between transmission directions. Therefore multirate transmission can be implemented.
- Channel reciprocity is also an interesting feature of TDD transmission. Due to fact the same channel spectrum is used in both transmission directions.
- A frame in the UTRA TDD mode lasts for 10 ms and is further divided in timeslots. Fig. 2.4.5 shows UTRA TDD frame structure.

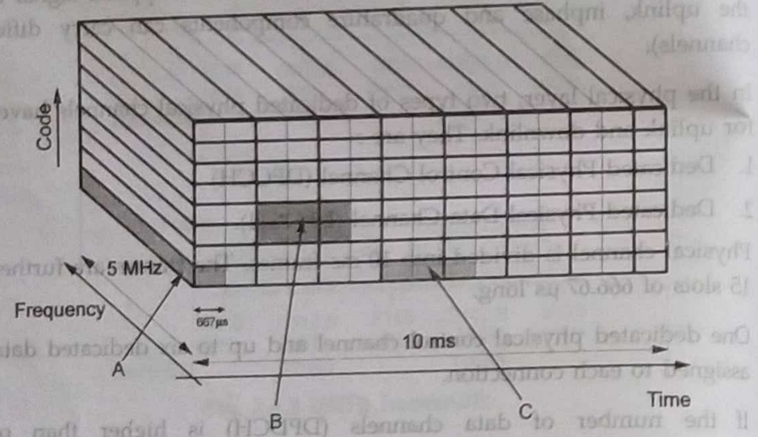


Fig. 2.4.5 UTRA TDD frame

2.4.1.8 Comparison of UTRA FDD and UTRA TDD Mode

	UTRA FDD	UTRA TDD
Multiple access method	CDMA	TDMA/CDMA
Duplex method	FDD	TDD
Channel bandwidth	5 MHz	
Chip rate	3.84 Mchip/s	
Frame length	10 ms	
Time slot structure	15 slots/frame	
Multirate method	Multicode, multislot and OVSF[a]	Multicode and OVSF[a]
Spreading (DL)	OVSF sequences for channel sep., truncated Gold seq. $(2^{18}-1)$ for cell and user sep.	
Spreading (UL)	OVSF sequences, truncated Gold seq. (2^{25}) for user separation	
Spreading factor	4-512	1-16
Channel coding	Convolutional coding (R=1/2, 1/3, K=9), turbo coding (8-state PCCC. R=1/3), service specific coding	
Interleaving	Inter-frame interleaving (10, 20, 40 and 80 ms)	
Modulation	QPSK	
Pulse shaping	Square-root raised cosine with roll-off factor = 0.22	
Detection	Coherent, based on pilot symbols	Coherent, based on midamble
Burst types	Not applicable	Traffic, random access and synchronization bursts
Dedicated channel power control	Fast closed loop (rate - 1500 Hz)	UL : open loop (100 or 200 Hz) DL : closed loop (≤ 800 Hz)
Intra-frequency handover	Soft handover	Hard handover
Inter-frequency handover	Hard handover	
Channel allocation	No DCA[b] required	Slow and fast DCA[b] possible
Intra-cell interference cancelation	Joint detection possible	Advanced receivers at base stations possible

OVSF - Orthogonal Variable Spreading Factor

DCA - Dynamic Channel Allocation

2.4.2 WCDMA

- **WCDMA** stands for **Wideband Code Division Multiple Access**, and is the 3G technology that employs the Direct-Sequence Code Division Multiple Access (DS-CDMA) 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 CDMA 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 working on the Unified Mobile Telecommunication Standard (UMTS) based on WCDMA.
- The other group is known as 3GPP2 works on CDMA2000.
- Organization 3rd Generation Partnership Project (3GPP) has continued that work by defining a mobile system that fulfills the IMT-2000 standard. This system called Universal Mobile Telecommunications System (UMTS).
- ITU finally approved a family of five 3G standards, which are part of the framework known as IMT-2000. These standards are :
  1) W-CDMA (UMTS 99)
  2) W-CDMA (HSPA)
  3) CDMA2000
  4) TD-CDMA
  5) TD-SCDMA

Generation	Technology	Data rate	Bandwidth	Data netwo
2G	GSM	9.6 or 14.4 kbps	200 kHz	Circuit Switche
2G	CDMA (1S-95)	9.6 or 14.4 kbps	1.25 MHz	Circuit Switche
2.5G	GPRS	128 kbps	200 kHz	Circuit/Packe
2.5G	Edge	384 kbps	200 kHz	Circuit/Packe
2.5G	CDMA2000-1XRTT	153 kbps	1.25 MHz	Circuit/Packe
3G	**WCDMA (UMTS 99)**	**384 kbps**	**5 MHz**	**Packet**
3G	**WCDMA (HSPA)**	**144 kbps, 384 kbps (5.76/14.4 Mbps)**	**5 MHz**	**Packet**
3G	CDMA2000-DO/EV	144 kbps, 384 kbps 2 Mbps	1.25 MHz	Packet
3G	TD-CDMA	144 kbps, 384 kbps 2 Mbps	5 MHz	Packet
3G	TD-SCDMA	144 kbps, 384 kbps, 2 Mbps	1.6 MHz	Packet

- WCDMA features two modes :

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

- W-CDMA does not need base station timing synchronization.
- WCDMA provides significant flexibility to provide support of multiple users at independent data rates. This flexibility necessitates the utilization of multiple complex waveforms for validation and test.

2.4.2.1 Parameters of WCDMA

1. Channel bandwidth : 5 MHz
2. Duplex mode : FDD and TDD
3. Spread spectrum technique : Direct spread
4. Chip rate : 3.84 MHz
5. Frame length : 10 ms (38400 chips/sec)
6. Slot length : 15 Slots per Frame (2560 chips/slot)
7. Spreading modulation : Balanced QPSK (downlink) and Dual-channel QPSK (uplink) with complex spreading circuit.
8. Data modulation : QPSK (downlink) and BPSK (uplink).
9. Channel coding : Convolutional code, Turbo code, and no coding.
10. Spreading factors : 4-256 (uplink) and 4-512 (downlink).
11. Modulation symbol rates vary from 960 K symbols/s to 15 K symbols/s (7.5 k symbols/s) for FDD uplink(downlink).
12. Spreading (downlink) : OVSF sequences for channel separation.
13. Gold sequences $2^{18}-1$ for cell and user separation (truncated cycle : 10 ms).
14. Spreading (uplink) : OVSF sequences for channel separation.
15. Gold sequences $2^{25}-1$ for user separation (truncated cycle : 10 ms).

2.4.2.2 WCDMA Channel

- Two channels of WCDMA are :
  1. Forward WCDMA channel
  2. Reverse WCDMA channel

2.4.2.3 Forward WCDMA Channel

- The forward channel is also called as transport channel.
- A forward WCDMA channel consists of a pilot channel, a synchronous chann paging channels and multiple forward traffic channels.
- Every channel is orthogonally spread by the suitable orthogonal function and s spread by a quadrature pair of PN sequence.
- The output of all the channels are added together and sent to modulator.
- The BS can operate in asynchronous fashion. Fig. 2.4.6 shows forward chann structure.

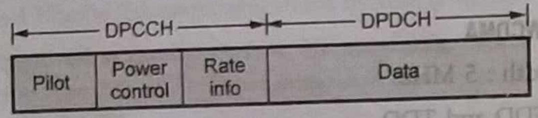


Fig. 2.4.6 Forward link channel structure in WCDMA

- The pilot signal is transmitted by BS to enable MS for clock recovery.
- The synchronous channel is transmitted by a base station to enable the MS obtain frame synchronization of WCDMA signal.
- The paging channel is transmitted by a BS to enable MS.
- The forward traffic channel is transmitted by a base station to enable the MS carry voice or data traffic.

2.4.2.4 Reverse WCDMA Channel

- In reverse traffic channel information bits and signaling information bits a processed separately.
- The channel multiplexing is done in modulator.
- Fig. 2.4.7 shows reverse link structure in WCDMA.

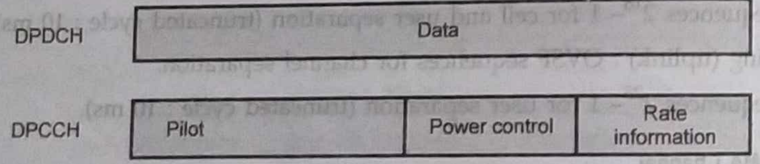


Fig. 2.4.7 Reverse link channel structure

2.4.3 CDMA2000

- Code division multiple access 2000 is the natural evolution of IS-95 (cdmaOne). I includes additional functionality that increases its spectral efficiency and data ra capability.

- Code Division Multiple Access 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 CDMA2000 standards are :
  1. cdma2000 1xRTT
  2. cdma2000 1xEV
  3. cdma2000 EV-DV
- cdma2000 1x supports both voice and data services over the standard 1.25 MHz CDMA channel. The 1x in the name signifies that it uses one 1.25 MHz channel. Due to improved modulation, power control, and overall design, it can achieve theoretical data transfer rates of 144 Kbps.
- There are two members of cdma2000 1x EV family :
  1. cdma2000 1x Evolution Data Optimized (cdma 1x EV-DO)
  2. cdma2000 1x Evolution Data and Voice (cdma 1x EV-DV)
- The cdma2000 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.
- cdma2000 EV-DV can offer data rates upto 144 kbps with about twice as many voice channels as IS-95B.
- Base station timing synchronization in cdma2000 can provide decreased latency and a reduced chance of dropping calls during soft handoff.
- Since both WCDMA and cdma2000 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 2000 proposals being developed by 3GPP and 3GPP2.

2.4.3.1 Network Components of CDMA2000

- Fig. 2.4.8 shows major components of CDMA 2000 wireless system.

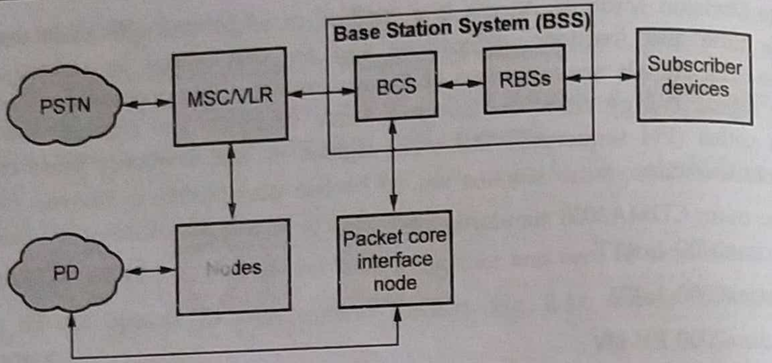


Fig. 2.4.8 Components of CDMA 2000

2.4.3.2 Network Nodes in CDMA2000

- Detail network nodes in a CDMA 2000 is shown in Fig. 2.4.9.

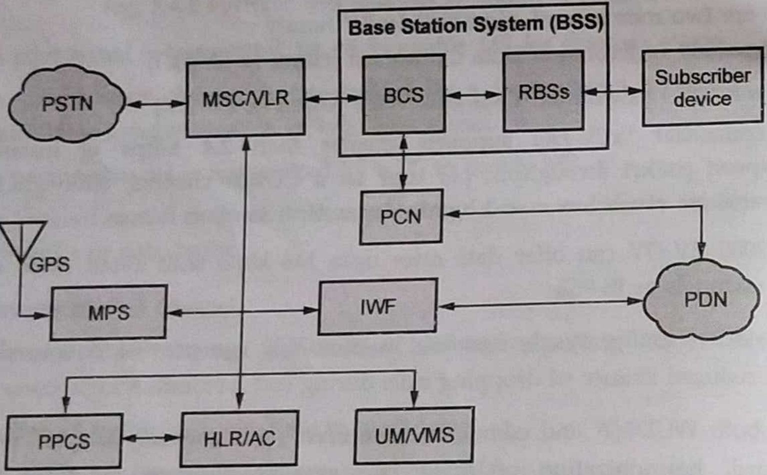


Fig. 2.4.9 Detail network nodes in CDMA 2000

Home Location Register/Authentication Centre (HLR/AC)

- The HLR holds the subscriber information in a database that is used by the system. It stores the ESN, subscribers service plan etc. AC provides secure database for authentication.

Base Station Subsystem (BSS)

- BSS consists of one BSC and all the radio base stations controlled by the BSC.

Base Station Controller (BSC)

- BSC interfaces between the MSC and the PCN, other BSS's in the system.

- It provides routing of data packets between the PCN and the RBS's, radio resource allocation, system and timing synchronization.

Radio Base Station (RBS)

- RBS interfaces between the BSC and the SD. Its functions include CDMA decoding and encoding of the subscriber, traffic and system overhead channels and the CDMA radio links to and from the subscriber.

2.4.3.3 Comparison of WCDMA and CDMA2000

Sr. No.	Feature	WCDMA	CDMA2000
1.	Chip rate	4.096 MCps	3.6864MCps
2.	Forward Link Pilot Structure	Dedicated Pilot with TDM	Common Pilot with CDM
3.	Base Station Timing	Asynchronous	Synchronous
4.	Frame length	10 or 20 ms optional	20 ms
5.	Forward link RF channel structure	Direct spread	Direct spread or multicarrier
6.	Spreading factor	4.096 mcps	3.6868 mcps
7.	Spreading modulation	QPSK	Uplink m-ary PSK downlink-QPSK

University Question

1. *What are the essential functional differences between 1st generation, 2nd generation and 3rd generation of networks ?* **GTU : Winter 2012, Marks 4**

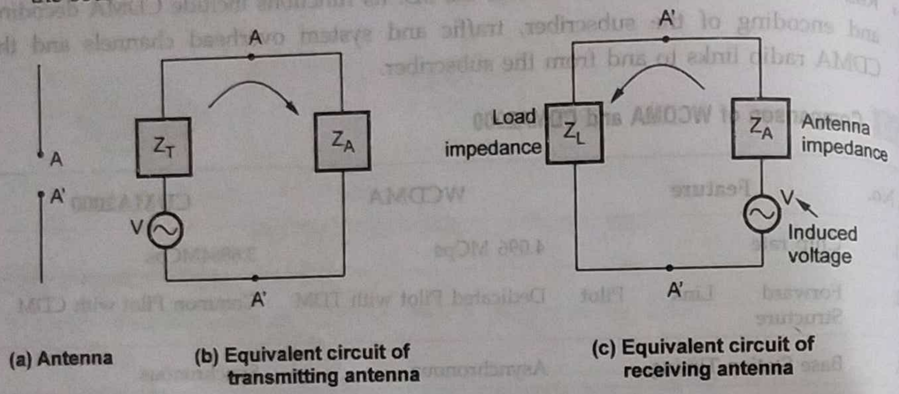
2.5 Antennas

2.5.1 Equivalent Circuit of Antenna

- Consider an antenna and its equivalent circuits for transmitter and receiver (setups). Let Z_A be the antenna impedance, Z_L be the load impedance and Z_T be the impedance at the transmitter end.
- At the transmitting end of antenna the power P_t originates and it radiates into the space. If an isotropic antenna source P_T is used then power available in spherical space could be measured as power/unit area. Such a power density is known as outward flow of the energy or the poynting vector 'e', in a given surface area.

$$\text{Poynting vector} = e = \frac{P_T}{4\pi r^2} \ W/m^2$$

- The power will be received by the receiver antenna that is at a distance 'r' from the source antenna and with aperture A.



(a) Antenna (b) Equivalent circuit of transmitting antenna (c) Equivalent circuit of receiving antenna

Fig. 2.5.1 An antenna with equivalent circuits

The received power is = $P_R = eA$

$$= \left(\frac{P_T}{4\pi r^2}\right) A \cdot \text{watt}$$

- The three antennas and its equivalent diagrams are shown here.

In the circuit,

$Z_T \rightarrow$ Transmitter impedance

$Z_A \rightarrow$ Antenna impedance

$V \rightarrow$ Voltage

A, A' → Antenna.

- A simple diagram of power received in space is shown here. The antenna is A-A' and it is at a distance 'r' from the source transmitting. The signal emerges in many directions as it propagates from source.

- The power received at receiving antenna is P_R watts measured as above.

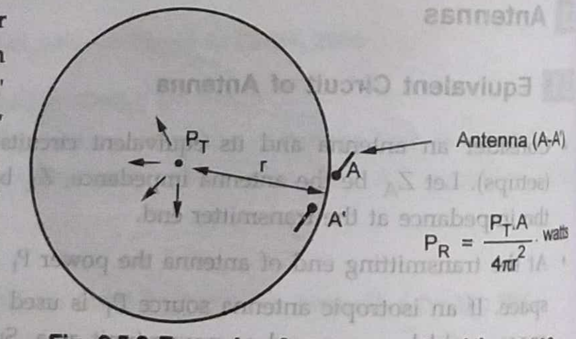


Fig. 2.5.2 Example of power received in space

The gain G and antenna aperture are related in the equation,

$$G = \frac{4\pi A}{\lambda^2}$$

where λ is the wavelength in 'm'.

The gain G is unity for a short dipole.

$$\text{Then} \quad \frac{4\pi A}{\lambda^2} = 1$$

$$\text{Aperture is} \quad \boxed{A = \frac{\lambda^2}{4\pi}}$$

Now substituting the value of antenna aperture in the equation of received power 'P_R', we get,

$$P_R = eA = \frac{P_T \ A}{4\pi r^2}$$

$$= \frac{P_T}{4\pi r^2} \cdot \frac{\lambda^2}{4\pi} = \frac{P_T \cdot \lambda^2}{(4\pi r)^2}$$

$$P_R = \frac{P_T}{(4\pi r/\lambda)^2}$$

2.5.2 Gain and Pattern Relationship

2.5.2.1 Antenna Gain

- **Antenna gain** is a gain relative to a reference antenna (isotropic radiator). Antenna gain is a measure of directional capabilities and efficiency of antenna.
- Antenna gain is defined as the ratio of the radiation intensity in a given direction to the radiation intensity by a reference (isotropic) antenna for similar power input to both antenna. The reference antenna can be short dipole or horn antenna whose gain can be calculated. Usually reference antenna is lossless isotropic source.

$$\text{Antenna gain } G(\theta, \phi) = \frac{P(\theta, \phi)}{P_{acc} / 4\pi r^2}$$

where P_{acc} is the total power accepted by the antenna from the transmitter (watts) and $\mathbf{P}_{acc}$ is radiated power density if all the $4\pi r^2$ power is radiated isotropically (watts/metre^2).

- The power accepted by the antenna is greater than the actual radiated power because of reflection (mismatch) efficiency and polarization loss factor.
- Antenna gain can be expressed interms of electric field.

$$G(\theta, \phi) = \frac{4\pi \text{ (Maximum radiated intensity)}}{\text{Total power radiated}}$$

$$G(\theta, \phi) = \frac{E^2_{max}\ (\theta_m, \phi_m)}{E^2\ (\theta, \phi)} \qquad \text{...(2.5}$$

where,

E represents electric field

E_{max} represents maximum value of E.

E^2 represents average value of E^2 which is related to radiation intensity.

θ, ϕ represents radiation angles on azimuth and elevation planes.

- The antenna pattern E can be obtained either by measurement or in analytic fo The antenna gain G is calculated from E pattern.

Effective Radiated Power

When the gain of an antenna is multiplied by its power input, the result is terme Effective Radiated Power (ERP).

2.5.2.2 Pattern and Gain of an Antenna Array

- In certain communication systems a highly directive beam of radiation is nee The conventional antennas and other elementary radiators cannot provide the highly directive beam of radiation because of low gain. This can be achieved by antenna arrays.
- An **antenna array** is a transmitting system consists of group of radiators arranged in specific manner.
- All the radiating elements of the arrays are placed close to each other so that they are within the

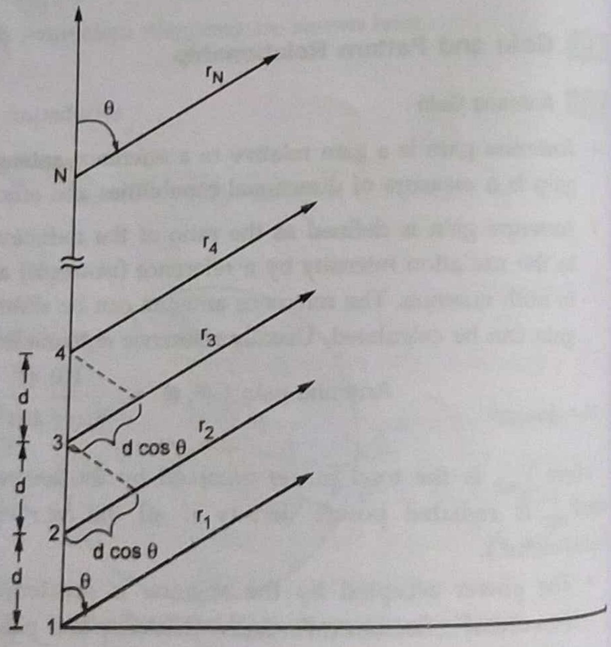


Fig. 2.5.3 Antenna array arrangement

induction field of each other. They interact with each other so that the resulting radiation pattern is the vector sum of individual patterns. The resulting radiation pattern is dependent on the characteristics of individual elements and the spacing between them. The antenna array also provides higher gain to the antenna.

- A simple and most practical array can be formed placing the radiating elements along a line. Fig. 2.5.3 shows N isotropic radiators forming an array. All the sources are equally spaced.
- The general field pattern of an antenna array is given as :

$$E(\theta, \phi) = \frac{\sin[N\pi(d\cos\phi \cdot \sin\theta + \psi]}{N\sin[\pi(d\cos\phi \cdot \sin\theta + \psi]} \times \begin{pmatrix}\text{Individual antanna} \\ \text{element pattern}\end{pmatrix} \qquad \text{...(2.5.2)}$$

where,

N represents number of elements in an array.

d represents spacing between adjacent elements in wavelength.

ψ represents phase difference between two adjacent elements.

θ, ϕ represents radiation angles.

θ = 90° for direction perpendicular to array axis.

- The gain of an array can be obtained by substituting equation (2.5.2) in equation (2.5.1).

2.5.2.3 Beamwidth

- Usually a directional antenna emits a beam of radiation in one or more directions. Various parts of radiation patterns are referred as **Lobes**.

1. Major Lobe :

- It is the radiation lobe in the direction of maximum radiation.

2. Minor Lobe :

- These are the lobes other than major lobe. A minor lobe is radiation in undesired direction hence it should be minimized.

3. Side Lobe :

- It is the lobe in any direction other than the major or intended lobe.

4. Back Lobe :

- It is a radiation whose axis makes an angle of approximately 180° with respect to beam of antenna.

- The **beamwidth of an antenna** is defined as the angle between its half pow points in major lobes. These are also the points where power density is 3 dB le than it is at its maximum point.

2.5.2.4 Relation between Gain and Bandwidth

- Assuming gain G and directivity D are same,

$$\boxed{G = (D) = \frac{32{,}400}{\phi^\circ\,\theta^\circ}} \quad \text{For small } \phi \text{ and } \theta$$

where, ϕ° and θ° are 3 dB beamwidths in two planes.

$$\boxed{G = \frac{41{,}253}{\phi^\circ\,\theta^\circ}} \quad \text{For large } \phi^\circ \text{ and } \theta^\circ$$

2.5.3 Antenna at Cell Site

2.5.3.1 For Coverage Use - Omnidirectional Antennas

- The Omnidirectional antennas have the characteristics of radiating uniformly i directions. The standard high gain omnidirectional antennas are 6 dB and 9 gain antennas. It is always suggested that in a startup cellular sys omnidirectional antennas should be used. Some of detailed design features handling a start-up system configuration are discussed here.

2.5.3.2 Start-up Cellular System Configuration

- For omnicells in start-up systems the cell-site antennas should be omnidirection Every transmitting antenna has to be capable of transmitting sign simultaneously from 16 transmitters with the help of a channel combiner. general every cell will have three transmitting antennas that could serve 45 voi transmissions at a time.
- Channel amplifiers are used for amplifying its own signal that has to be se After 16 radio signals (16 channels) are passed through the channel combiner un at the receiving end, two antennas can receive all the 45 voices which we transmitted.
- In case two identical signals are received by these two receiving antennas th they would be sent to the diversity receiver of the corresponding channel. Th receiving the different voice signals is done.

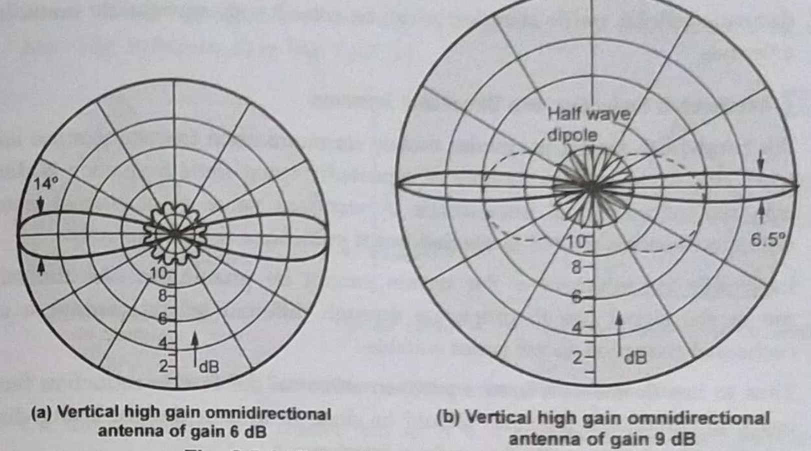


Fig. 2.5.4 High-gain omnidirectional antenna

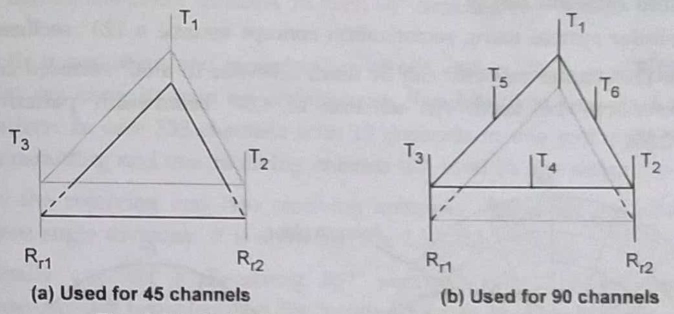


Fig. 2.5.5 Cell-site antennas used for omnicells

2.5.3.3 Abnormal Antenna Configuration

- In cellular mobile system if the number of subscribers increase there will be more call traffic. In particular some cells would require more channels than other cells to meet the increasing call traffic. In general the omnicells will be provided with 90 voice channels.

  90 voice channels - six antennas (T_1 to T_6) have to be used.

  45 voice channels - three antennas (T_1 to T_3) have to be used.
- But though the number of transmitting antennas are more the receiving antennas are only two. The complexity of having more number of transmitting antennas can be reduced by using a ring combiner. For example, in this case if a ring combiner capable of combining two 16 channel signals is used then it is enough to use only three transmitters for 90 channels case instead of six transmitters and thus the

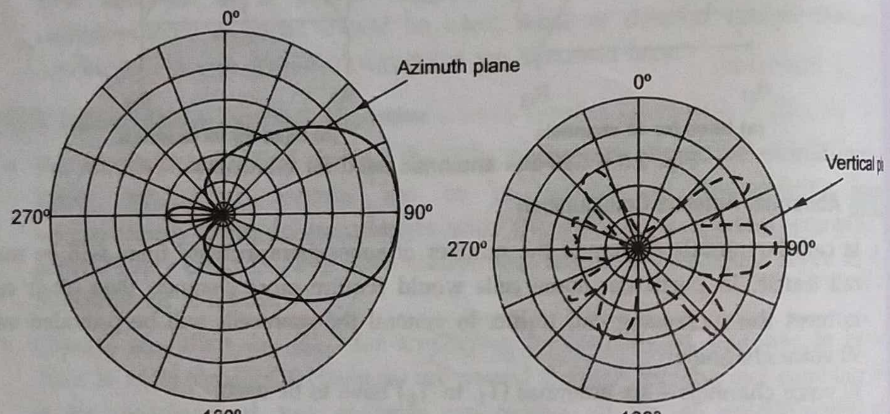
dynamic cellular traffic complexity can be solved with appropriate omnidirectio antennas.

2.5.3.4 Interference Reduction with Directional Antennas

- For bandwidth saving in cellular mobile communication frequency reuse concep used. But when reuse technique of repeatedly using same frequency is done t is a risk of cochannel interference. A standard value of cochannel interfere reduction factor q = D/R is applied but it suits for a flat terrain only.
- In mobile environment a flat terrain cannot be guaranteed. As the subsc moves the signal has to propagate through different terrain contour a stan cochannel reduction factor is not suitable.
- Thus to handle the interference problem either an increase in reduction factor usage of directional antennas should be done in system design. Using direct antennas is a better method to reduce interference.

1. Directional Antenna Setup

- In cellular system using sectorization concept assume a 120° sectored cell. For cell a 120° corner reflector can be used. Likewise in a 60° sectored cell a 60° co reflector can be used. An antenna of 120° beamwidth pattern is show Fig. 2.5.6.



(a) Azimuth pattern

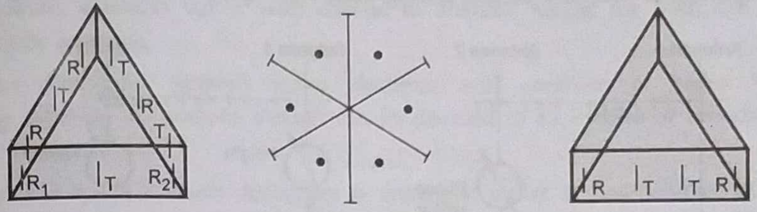
(b) Vertical pattern

Fig. 2.5.6 8 dB directional antenna pattern

2. Normal Antenna System Configuration

- If the cluster size N = 7 pattern then it means the 120° sectored cell. If freque reuse technique is applied in this cell then 333 channels can be used here. Ev

sector of 120° is capable of serving 16 channels with one transmitting and two receiving antennas, as in Fig. 2.5.7 (a).



(a) 120° sector for 45 channels

(b) 60° sector

(c) 120° sector for 90 channels

Fig. 2.5.7 Directional antennas for different sectors

- On the otherhand if a cluster size of N = 4 pattern is used, 60° sectored cell is considered. For omni cell systems the cluster size of N = 4 cannot be used because of its inadequate reuse distance. In such 60° sectored cell two different approaches are used.

i. Both transmitting and receiving are of 60° sectors. Each sector has an antenna that can carry its own set of frequency channels. It is known as N = 4 cellular pattern. In case 333 channels with 13 channels in one sector are used then one transmitting and one receiving antenna are used in one sector.

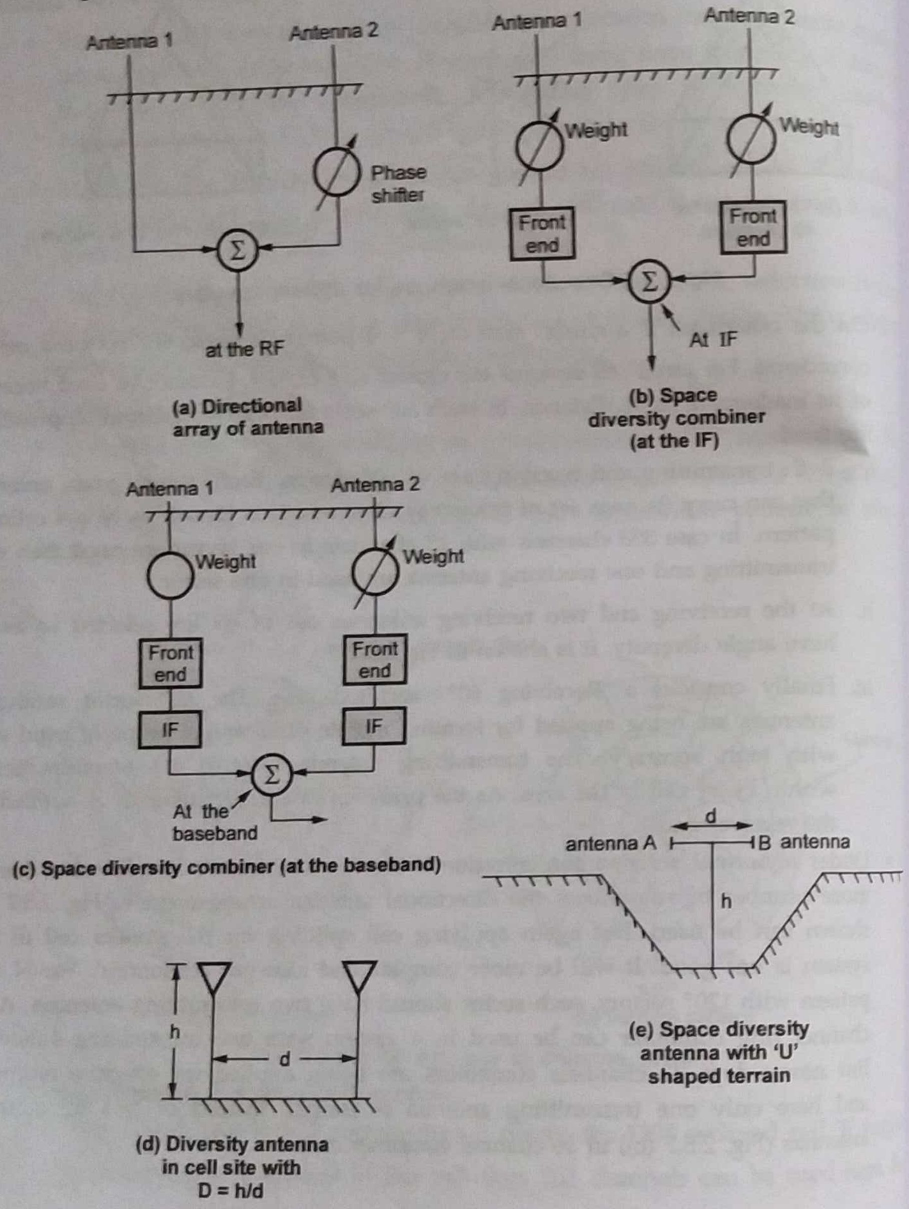
ii. At the receiving end two receiving antennas out of six are selected so as to have angle diversity. It is shown in Fig 2.5.7 (b).

iii. Finally consider a 'Receiving 60°' sectored case. The 60° sector receiving antennas are being applied for locating mobile units and it properly hand offs with high accuracy. The transmitting antenna systems are omnidirectional within every cell in the area. As the previous case angle diversity is applied at the receiver end.

- Under abnormal antenna configuration if there is an increase in call traffic due to more number of subscribers the directional antenna arrangement in Fig. 2.5.7 (c) shown can be used. But again applying cell splitting for the smaller cell in the system is not good. It will be more complex and also not economical. For N = 7 pattern with 120° sectors, each sector should have two transmitting antennas. A 16 channel ring combiner can be used in a system with two transmitting antennas. But now-a-days 32 channels combiners are being applied for effective reception and here only one transmitting antenna is enough instead of two transmitting antennas (Fig. 2.5.7 (c)) in 16 channel combiner case.

3. Space-Diversity Antennas at Cell Site

- The diversity techniques, provide two or more number of inputs at the mob reception end such that fading among these two inputs are not correlated.



(a) Directional array of antenna

(b) Space diversity combiner (at the IF)

(c) Space diversity combiner (at the baseband)

(d) Diversity antenna in cell site with D = h/d

(e) Space diversity antenna with 'U' shaped terrain

Fig. 2.5.8 Space diversity antenna concepts

- In space diversity technique two antennas are separated by a distance 'd' so as to get the two input signal with low correlation among fading effects. The antenna would be at a height of 'h' from ground level at the cell site. As the distance 'd' between antennas varies with change in antenna height for both cell site and mobile antenna.
- The directional antenna array elements will combine at radio frequency Fig. 2.5.8 (a). Its antenna pattern can be directed to an endfire or broadside array by design.
- But the space diversity technique is combined either at baseband or at IF as in Fig. 2.5.8 (b) and (c). For combining either maximal ratio combining or the equal-gain technique can be applied. Equal gain combining technique can co-phase the random phase of all individual branches at IF level.
- The Maximal ratio combining can obtain maximum SNR at the output of IF. The summation of power outputs at baseband is equivalent to the maximal ratio combining method.
- The switch combined technique uses one RF signal only at a time for desired output signal. Also the selection-combined technique can select the strongest signal available among the inputs of two antennas.
- A simple two-branch diversity antenna with spacing 'd' is shown in Fig. 1.3.8 (d). It receives the same signal but with different fading envelopes, with different antenna.

> Degree of correlation between two fading signals ∝ Degree of separation distance between antennas.

- The fading is somewhat reduced when the two fading envelopes are combined.

$$\eta = \frac{h}{d}; \quad h \rightarrow \text{height of antenna}, \quad d \rightarrow \text{separation distance}$$

Sr. No.	Separation distance 'd'	Antenna height required
1.	$d \geq 14\lambda$	150 feet (50 m)
2.	$d \geq 8\lambda$	100 feet (30 m)

- In an omnicell the two space-diversity antennas has to be aligned with the terrain area. It should have a 'U' shape as in Fig. 2.5.8 (e).

- The space-diversity antennas separates only horizontally and hence horizontal separation should be done in the design. Comparing to other diversity antennas space diversity antenna configuration reduces fading in mobile transmissions.

4. Umbrella Pattern Antennas

- In cell-site antennas used in mobile communication can be umbrella pattern antennas. For certain situations these antennas are much useful to meet the mobile traffic in busy hours.
- There are many types of umbrella pattern antennas available. They are

i) Broadband umbrella-pattern antenna.

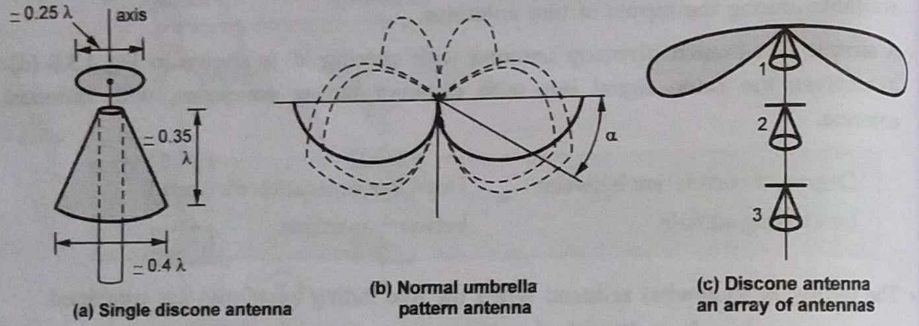
ii) Normal umbrella-pattern antenna.

iii) High-gain broadband umbrella-pattern antenna.

iv) Interference reduction antenna.

i) Broadband umbrella-pattern antenna

- Consider a bioconical antenna. One of its cones is extended to 180° so as to form a disk. It is called as discone antenna and acts as broadband umbrella-pattern as shown in Fig. 2.5.9 (a).



(a) Single discone antenna

(b) Normal umbrella pattern antenna

(c) Discone antenna an array of antennas

Fig. 2.5.9 Umbrella pattern antennas

ii) Normal umbrella-pattern antenna

- The energy present in confined area should be controlled and for this an umbrella-pattern antenna (Fig. 2.5.9 (b)) can be designed, by using a monopole with top disk (top-loading) arrangement. The tilting angle of the radiation pattern is determined by the size of the top disk used. They are inversely proportional.
- If a larger disk is used as top disk, smaller will be the tilting angle of the pattern. If a smaller disk is used as top disk of monopole, then larger will be the tilting angle.

iii) High-gain broadband umbrella-pattern antenna

- A vertical stacking of number of umbrella-pattern antennas forms a high-gain antennas applicable for mobile transmissions.

- If M is the number of antenna elements, ϕ is the direction of the wave travel and 'd' is the spacing observed between elements then E_0 for one umbrella pattern will be

$$E_0 = \frac{\sin\left(\frac{Md}{2\lambda}\right) \cdot \cos\phi}{\sin\left(\frac{d}{2\lambda}\right) \cdot \cos\phi}$$

- All the above umbrella pattern antennas are useful in increasing coverage for wireless communication.

iv) Interference reduction antenna

- The parasitic elements can be used for antenna configurations to reduce interferences. Here the parasitic elements are longer (1.05 times approx) than the active element so that reduction in interference is observed.

Minimum separation of cell-site receiving antennas

- To avoid the intermodulation problems the separation distance 'd' between two transmitting antennas has to be minimized. In addition to this receiver desensitization is also minimized by reducing separation distance between transmitting and receiving antennas.
- Consider a space-diversity receiver unit where two receiving antennas are used. The antennas are placed with minimum separation distance. There will be near-field disturbance generation because of the close spacing and ripples formed in the radiation patterns as shown in Fig 2.5.10.

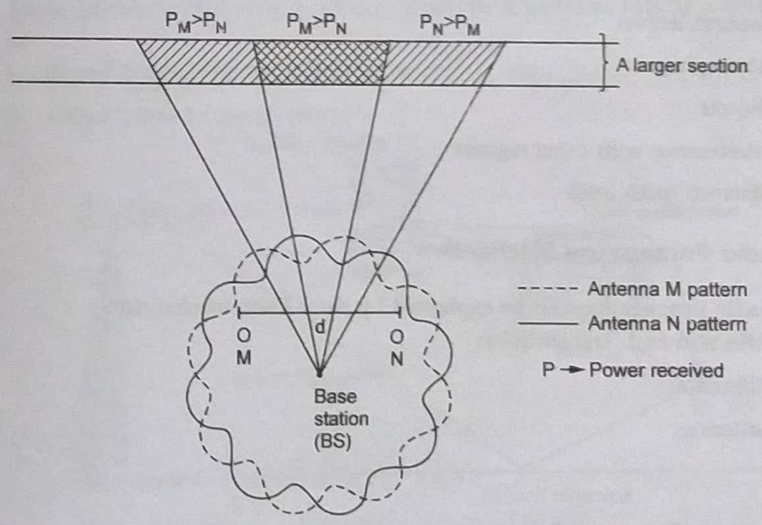


Fig. 2.5.10 Antenna pattern of antennas M, N

- The difference in the received power at different angle for the antennas M and are shown in the antenna pattern.
- The difference in the power received at a point for the two antennas will be h if the antennas are closely spaced. This power reception now is not only confin to a smaller sector but a large area (a section of road) is noted. Now fading can be reduced by using space diversity antennas due to close spacing.
- For a separation distance of 8λ between the two receiving antennas at 850 M frequency there will be a ± 2 dB power difference and it is tolerable for obtain reasonable voice quality. If the antennas at receiver are not closely spaced, fad can be controlled.

2.6 Mobile Radio Propagation

- The radio channel is different than wired channel. There exists extremely h environment compared to "wired" or guided media.
- The radio channel is time variant because of movement of people, switching and on of interference, movement of mobile terminals, sensitivity to a variety other factors, fading and multipath. Therefore, there is need of a framework characterizes the radio channel.

Radio channel characterization

- The radio propagation is modeled as a random phenomenon. Transmission radio signals are effected by :
  1. Ground terrain
  2. Atmosphere
  3. Objects
  4. Interference with other signals
  5. Distance (path loss)

2.6.1 Radio Propagation Mechanism

- The radio propagation can be explained by three basic mechanisms :
  1. Reflection and transmission
  2. Diffraction
  3. Scattering.

2.6.1.1 Reflection and Transmission

- Reflection occurs when electromagnetic wave impinges on object larger than the wavelength λ. The electromagnetic wave bounces off the object. Examples : Walls, buildings, ground.
- The electromagnetic signal is attenuated by a reflection factor. Attenuation depends on -
  1. Nature of material
  2. Frequency of the carrier
  3. Angle of incidence
  4. Nature of the surface.
- Usually transmission through an object leads to larger losses (absorption) than reflection. Multiple reflections can result in a weak signal.

2.6.1.2 Diffraction

- Diffraction occurs when radio wave is incident upon the edge of a sharp object. Examples : Wall, roof edge, door.
- Each such object becomes a secondary source of emission. In this case, the losses are much larger than with reflection or transmission.
- Diffraction is important in micro-cells for non-line of sight transmission i.e. propagation into shadowed regions.
- Diffraction is not significant in indoor areas because of large losses in diffracted signal.

2.6.1.3 Scattering

- Scattering is caused by irregular objects comparable in size to the wavelength. These objects scatter rays in all directions. Each scatterer acts as a source resulting in -
  1. Signal propagates in all directions
  2. Large losses in signal strength

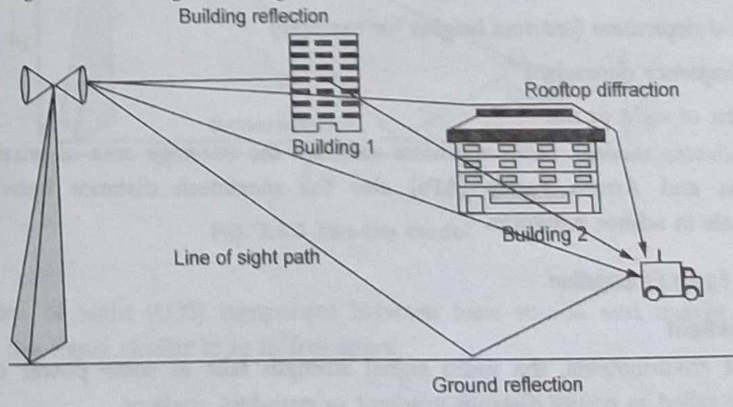


Fig. 2.6.1 Radio propagation mechanisms in an outdoor area

3. Insignificant except when the transceiver is in very cluttered environments

- Examples of scatterers : Foliage, furniture, lampposts, vehicles.
- Fig. 2.6.1 and Fig. 2.6.2 illustrates all three mechanisms for outdoor and indoor applications.

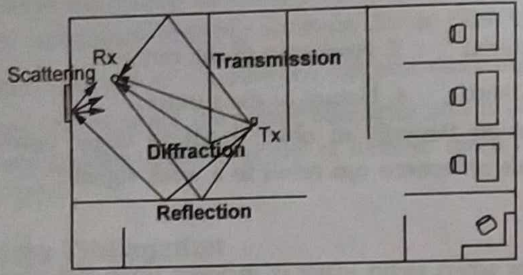


Fig. 2.6.2 Radio propagation mechanisms in an indoor area

2.6.2 Path Loss Modeling and Signal Coverage

- Path-loss models are commonly used to estimate link budgets, cell sizes and shapes, capacity, handoff criteria etc.
- The path-loss models used to estimate macroscopic or large scale variation of Received Signal Strength (RSS).

Path-loss = Loss in signal strength as a function of distance

- Path loss is :
  1. Terrain dependent (urban, rural, mountainous), ground reflection, diffraction etc.
  2. Site dependent (antenna heights for example)
  3. Frequency dependent
  4. Line of sight or not
- By path-loss models, radio engineers calculate the coverage area of wireless base stations and Access Points (APs) also the maximum distance between two terminals in ad-hoc networks.

2.6.2.1 Free Space Propagation

Path-loss Gradient

- In most environments, the radio signal strength falls as some power α of the distance called as power distance gradient or path-loss gradient.

- The signal strength is proportional to $P_t\, d^{-\alpha}$, where P_t is transmitted power and d is distance in meters.
- When an antenna radiates signal in all direction, the signal strength density at a sphere of radius d is the total radiated signal strength divided by the area of the sphere ($4\pi d^2$). Also, there are losses dependent on frequency.
- The relation between transmitted power (P_t) and received power (P_r) is given by :

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$

where,

G_t = Transmitter antenna gain in the direction from transmitter to receiver

G_r = Receiver antenna gain

d = Distance between transmitter and receiver

λ = Wavelength of carrier

2.6.2.2 Two-Ray Model of Mobile Environment

- In free space, the signal travels from the transmitter to receiver along the single path but in realistic environment, the signal reaches the receiver through several different paths.
- The two-ray model is shown in Fig. 2.6.3.

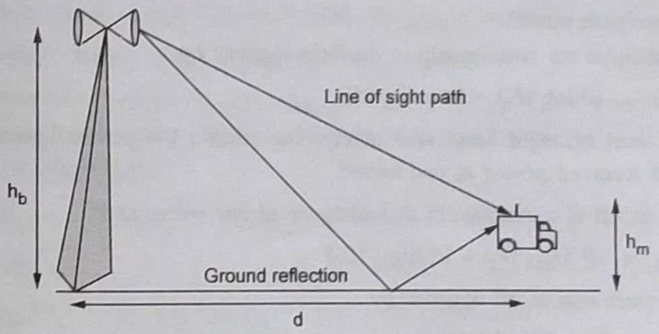


Fig. 2.6.3 Two-ray model

- The Line of Sight (LOS) component between base station and mobile terminal carries the signal similar to as in free space.

- Another path of signal is through the reflection off the earth's surface. These t paths travel different distances based on height of base station antenna (h_b) a height of mobile terminal antenna (h_m).
- At receiver these two signals and added constructively or destructively. T relation between transmit power for two-ray model can be approximated b expression :

$$P_r = P_t G_t G_r \frac{h_b^2 h_m^2}{d^4}$$

- It can be observed that the signal strength falls as the fourth power of distance between the transmitter and receiver. In other words, there is a loss of 40 dB p decade or 12 dB per octave.

2.6.2.3 Distance Power Relationship and Shadow Fading

- The received signal power (P_r) is proportional to the distance between transmi and receiver (d), raised to certain exponent α which is referred to distance-power gradient.

$$P_r = P_0 \, d^{-\alpha}$$

where,

P_0 = Received power at reference distance from transmitter (usually one meter).

α = 2; for free space and

α = 4; for two-path model.

- The distance power relationship in decibels is given by :

$$10 \log (P_r) = 10 \log (P_0) - 10 \alpha \log (d)$$

- The last term on right hand side of equation shows the power loss in dBs w respect to received power at one meter.
- Path loss in dB at a distance of at a distance of one meter as :

$$L_0 = 10 \log_{10} (P_t) - 10 \log_{10} (P_0)$$

- The total path loss in dB is given by :

$$L_p = L_0 + 10 \alpha \log(d)$$

where,

L_0 is termed the frequency dependent component.

Parameter α is called the "path loss gradient" or exponent.

The value of α determines how quickly the RSS falls with distance.

2.6.2.4 Shadow Fading

- Shadowing occurs when line of site is blocked. The actual received signal strength will vary around its mean value. The shadow fading is also called as slow fading.
- The path loss equation can be modified to include this effect by adding a random component.

$$L_p = L_0 + 10 \alpha \log_{10} (d) + X$$

where,

X is random signal with a distribution that depends on fading component.

2.6.2.5 Path-Loss Models for Megacellular

- The megacellular area spans over 100s of kilometres. The mega cellular areas are served mostly by LEO satellites.
- The path loss is usually modelled similar to free space but fading characteristics are different.

2.6.2.6 Path-Loss Models for Macrocellular Areas - Okumura-Hata Model

- Empirical formula calculating the median path-loss for a quasi smooth terrain in an urban area is -

$$L_p = 69.55 + 26.16 \log f_c - 13.82 \log h_b - a(h_m) + [44.9 - 6.55 \log h_b] \log d$$

where,

f_c in MHz : $150 < f_c < 1500$ MHz

h_b in meters - base station antenna height : $30 < h_b < 200$ m

h_m in meters - mobile antenna height : $1 < h_m < 10$ m

d in kilometers - distance : $1 < d < 20$ km

- The correction factor for the mobile antenna height is given by :

1. Small-medium city :

$$a(h_m) = (1.1 \log f_c - 0.7)\, h_m - (1.56 \log f_c - 0.8)$$

2. Large city :

$$a(h_m) = 8.29 (\log 1.54\, h_m)^2 - 1.1, \quad f_c \leq 200 \text{ MHz}$$

$$a(h_m) = 3.2 (\log 11.75\, h_m)^2 - 4.97, \quad f_c \leq 400 \text{ MHz}$$

3. For a suburban area :

$$L_p = L_p(\text{Urban}) - \left[2\log\left[\frac{f_c}{28}\right]^2 - 5.4 \right]$$

For an open area :

$$L_p = L_p(\text{Urban}) - 4.78 (\log f_c)^2 + 18.33 \log f_c - 40.94$$

2.6.2.7 Path-Loss Models for Microcellular Areas

- The microcellular area spans from 100 meters to few of kilometres. These usually supported by base station height which is approximately equals to tops or lampposts.
- The propagation characteristics are quite complex wi'h the propagation of sig affected by reflection from buildings, grounds and sca 'ering from vehicles.

2.6.2.8 Path-Loss Models for Picocellular Indoor Areas

- The picocells are radio cells covering buildings or parts of buildings. The pi spanning between 30 and 100 m.
- The applications of picocells are : WLANs, wireless PBX, PCS

Multifloor Attenuation Model

- Multifloor attenuation model is expressed as -

$$L_p = L_0 + nF + 10 \log(d)$$

where,

F is signal attenuation per floor.

L_0 is the path-loss at first meter.

d is distance in meters.

n is number of floors.

- Typical values for F = 10 dB and 16 dB for measurements at 900 MHz 1.7 GHz, respectively.
- Furniture objects cause shadowing approximately of 4 dB.

2.6.2.9 Path-Loss Models for Femtocellular Area

- The femtocellular area span is between 2 and 10s of meters.
- The femtocells exist in individual residences using low power devices applications : bluetooth, home RF. Since femtocells are usually deployed residential areas, JTC model may apply to predict the coverage of femtoce 1.8 GHz. For operation at 2.4 GHz and 5 GHz (unlicensed bands) -

$$L_p = L_0 + 10\, \alpha \log(d)$$

where,

L_0 is the path-loss at first meter.

d is distance in meters.

α is the path-loss exponent.

- Selected measurements of indoor path loss models are shown in Table 2.6.1.

f_c (GHz)	Environment	Scenario	Path Loss at d = 1 m (dB)	Path loss gradient α
2.4	Indoor office	LOS	41.5	1.9
		NLOS	37.7	3.3
5.1	Meeting room	LOS	46.6	2.22
		NLOS	61.6	2.22
5.2	Suburban residences	LOS and same floor	47	2 to 3
		NLOS and same floor		4 to 5
		NLOS and room in the higher floor directly above Tx		4 to 6
		NLOS and room in the higher floor not directly above the Tx		6 to 7

Table 2.6.1 Path-loss models for femtocells at 2.4 GHz, 5.1 GHz and 5.2 GHz

2.6.3 Effects of Multipath and Doppler

- Radio waves arrive at the receiver from different directions with different delays. At the receiver antenna they combine via vector addition.
- Received signal level varies (10s of dBs) due to short-term (rapid) variations and long-term (slow) variations.
- Rapid fluctuation is caused by :
  1. Movement of mobile terminal toward or away from the base station transmitter is called as Doppler.
  2. Addition of signals arriving via different paths called as multipath fading.

For an open area :

$$L_p = L_p(\text{Urban}) - 4.78 (\log f_c)^2 + 18.33 \log f_c - 40.94$$

2.6.2.7 Path-Loss Models for Microcellular Areas

- The microcellular area spans from 100 meters to few of kilometres. These usually supported by base station height which is approximately equals to tops or lampposts.
- The propagation characteristics are quite complex with the propagation of sig affected by reflection from buildings, grounds and scattering from vehicles.

2.6.2.8 Path-Loss Models for Picocellular Indoor Areas

- The picocells are radio cells covering buildings or parts of buildings. The pi spanning between 30 and 100 m.
- The applications of picocells are : WLANs, wireless PBX, PCS

Multifloor Attenuation Model

- Multifloor attenuation model is expressed as -

$$L_p = L_0 + nF + 10 \log(d)$$

where,

F is signal attenuation per floor.

L_0 is the path-loss at first meter.

d is distance in meters.

n is number of floors.

- Typical values for F = 10 dB and 16 dB for measurements at 900 MHz 1.7 GHz, respectively.
- Furniture objects cause shadowing approximately of 4 dB.

2.6.2.9 Path-Loss Models for Femtocellular Area

- The femtocellular area span is between 2 and 10s of meters.
- The femtocells exist in individual residences using low power devices applications : bluetooth, home RF. Since femtocells are usually deployed residential areas, JTC model may apply to predict the coverage of femtoce 1.8 GHz. For operation at 2.4 GHz and 5 GHz (unlicensed bands) -

$$L_p = L_0 + 10 \alpha \log(d)$$

where,

L_0 is the path-loss at first meter.

d is distance in meters.

α is the path-loss exponent.

- Selected measurements of indoor path loss models are shown in Table 2.6.1.

f_c (GHz)	Environment	Scenario	Path Loss at d = 1 m (dB)	Path loss gradient α
2.4	Indoor office	LOS	41.5	1.9
		NLOS	37.7	3.3
5.1	Meeting room	LOS	46.6	2.22
		NLOS	61.6	2.22
5.2	Suburban residences	LOS and same floor	47	2 to 3
		NLOS and same floor		4 to 5
		NLOS and room in the higher floor directly above Tx		4 to 6
		NLOS and room in the higher floor not directly above the Tx		6 to 7

Table 2.6.1 Path-loss models for femtocells at 2.4 GHz, 5.1 GHz and 5.2 GHz

2.6.3 Effects of Multipath and Doppler

- Radio waves arrive at the receiver from different directions with different delays. At the receiver antenna they combine via vector addition.
- Received signal level varies (10s of dBs) due to short-term (rapid) variations and long-term (slow) variations.
- Rapid fluctuation is caused by :
  1. Movement of mobile terminal toward or away from the base station transmitter is called as Doppler.
  2. Addition of signals arriving via different paths called as multipath fading.

2.6.4 Fading

- Fading is defined as variation in intensity of received radio signal due to :
  - Variation in propagation time
  - Relative phase differences
  - Change in frequencies
  - Change in characteristics of propagation path with time.
- Fading refers to time variation of received signal power caused by change transmission medium fading describes the rapid fluc ion of amplitudes, ph or multipath delays of radio signal over a short pe of time or travel dista The strength of received signal varies with respect to ti e.
- Various propagation mechanisms caused fading of radio signals such refraction, reflection, diffraction, scattering, attenuation and ducting of ra waves. These propagation mechanisms determine amplitude, phase, polariza and frequency of fading.
- Fading is caused by certain terrain geometry, attenuation, changes in transmis medium, refraction, multipath propagation, rainfall, obstacles etc.

2.6.4.1 Types of Fading

- Two types of fading exists in radio signals.
  1. Large scale / Long term fading / Slow fading
  2. Small scale / Short term fading / Fast fading

2.6.4.2 Large Scale Fading

- When fading duration is very long and signal attenuation is large it is called **large scale fading**. The large scale fading is due to several factors such atmosphere, large pathloss, shadowing, trees and foliage. Such kind of fading usual low observed in rural areas. This slowly changing fading is referred as sl **fading**.
- Large scale fading can be compensated by increasing transmitter power so t received signal can be within certain limits.

2.6.4.3 Small Scale Fading

- When fading duration is very small i.e. signal strength varies very fast for sh distance, it is called as **small scale fading**. Small scan fading mainly because multipath propagation, speed of surrounding obstacles, transmission bandwidth signal and doppler shift.
- The changes of amplitude is about 20 or 30 dB over a short distance. This rap changing fading phenomenon is referred as **fast fading** : (See Fig. 2.6.4 on n page).

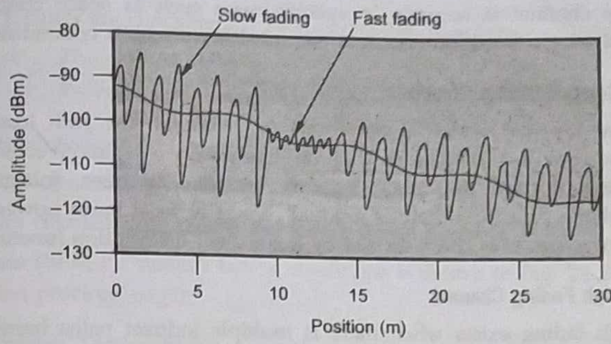


Fig. 2.6.4 Slow and fast fading in an urban mobile environment

2.6.4.4 Flat Fading

- When fading in all frequency components of received signal fluctuate in the same proportions simultaneously it is called as **flat fading**. It is also referred as non-selective fading.

2.6.4.5 Selective Fading

- When different spectral components of received radio signal fluctuates unequally it is called as **selective fading**.
- Selective fading is relative to the bandwidth of entire communical channel. Non-selective fading implies that the signal bandwidth of interest is narrower than the entire spectrum affected by fading.

2.6.5 Modeling of Multipath Fading

- For designing a communication system, the effects of multipath fading and noise on the communication channel must be estimated. The multipath fading channel can be divided on the basis of distribution function of the instantaneous power of the channel on the radio environment. Different types of fading multipath channel are as follows :
  1. Additive White Gaussian Noise (AWGN) channel
  2. Log normal fading channel. 3. Rayleigh fading channel
  4. Rician fading channel

2.6.5.1 AWGN Channel

- In AWGN channels, the desired signal is degraded by the thermal noise associated with the channel itself and losses in transmitter and receiver circuitry.

- AWGN channel is accurate in specific cases such as space communication a co-axial wire communication. It is not suitable for mobile communication.

2.6.5.2 Log Normal Fading Channel

- The propagation models a developed to determine the path loss are known large scale fading models as they all characterizes the received signal power averaging it over the large distance. But due to trees, foliage, rainfall, a atmospheric condition there is gradual change in local mean power and such ty of fading channel is characterized by log normal distribution function.

2.6.5.3 Rayleigh Fading Channel

- Rayleigh fading exists when there is multiple indirect paths between transmi and receiver i.e. there is no distinct Line Of Sight (LOS) path.
- Rayleigh fading can be dealt by studying performance characteristics in s critical environment.

2.6.5.4 Rician Fading Channel

- Rician fading exists where there is a direct Line Of Sight (LOS) path along w number of indirect multipath signals. This model is mostly applicable in ind environment whereas Rayleigh fading model characterizes outdoor environment

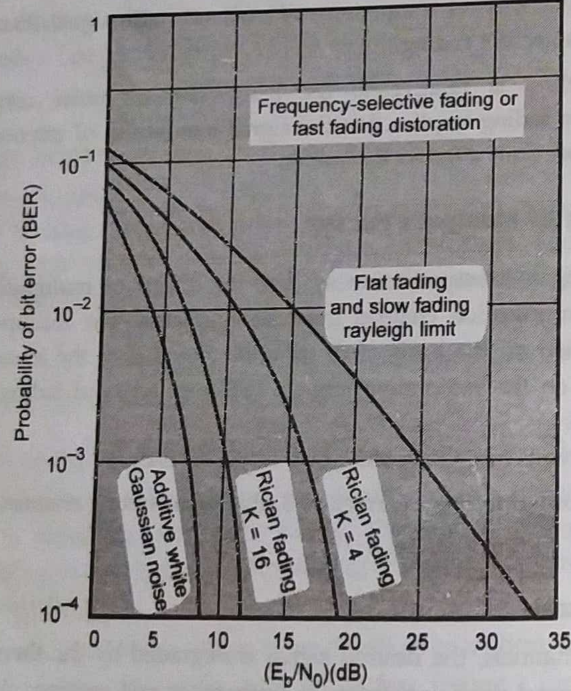


Fig. 2.6.5 Theoretical bit error rate for various fading conditions

- All the channels are characterized by a parameter 'K' where -

$$K = \frac{\text{Power in dominant path}}{\text{Power in scattered paths}}$$

i) For Rayleigh channel, numerator is zero therefore K = 0

ii) For AWGN channel, denometor is zero therefore $K = \infty$

iii) For Rician channel, with reasonably strong signal K = 4 to 16

Bit Error Rate (BER) for various fading conditions is shown in Fig. 2.6.5. (See Fig. 2.6.5 on previous page)

2.7 Modulation Techniques

- The important reasons for choosing different encoding techniques are:

1. Digital data, digital signal

- The equipments are less complex and expensive than digital-to-analog modulation equipment.

2. Analog data, digital signal

- This method permits use of modern digital transmission and switching equipments. Data needs to be converted to digital form.

3. Digital data, analog signal

- Here some transmission media will only propagate analog signals. E.g., unguided media. Needed to take advantage of existing transmission media that only allows the transmission of analog signal.

4. Analog data, analog signal

- Analog data in electrical form can be transmitted easily and cheaply.
- Modulation to shift the bandwidth of baseband signal to another portion of spectrum.
- Multiple signals on different position on the spectrum can share the same transmission medium (frequency-division multiplexing). It can be done with voice transmission over voice-grade lines.

2.7.1 Signal Encoding Criteria

- Signal encoding schemes can be compared on certain criteria such as :
  1. Signal Spectrum - Bandwidth requirement for a given data rate
  2. Clocking
  3. Signal interference and Noise immunity

4. Cost and complexity
5. Performance in an AWGN channel - How does the bit error rate vary wit energy per bit available in the system when white noise present
6. Performance in fading multipath channels
7. Cost - The modulation scheme needs to be cost efficient. Circuitry shoul simple to implement and inexpensive (e.g. detection, amplifiers)

2.8 Spread Spectrum

GTU : Winter-11, 13, 14, Summer-13, 14

- Spread Spectrum (SS) is a means of transmission in which:
  1. The transmitted signal occupies a bandwidth which is much greater tha minimum necessary to send the information.
  2. Spreading is accomplished by means of a spreading signal called a 'code' si which is independent of the data.
  3. At the receiver, de-spreading is done by correlating the received SS signal a synchronized replica of the spreading signal.

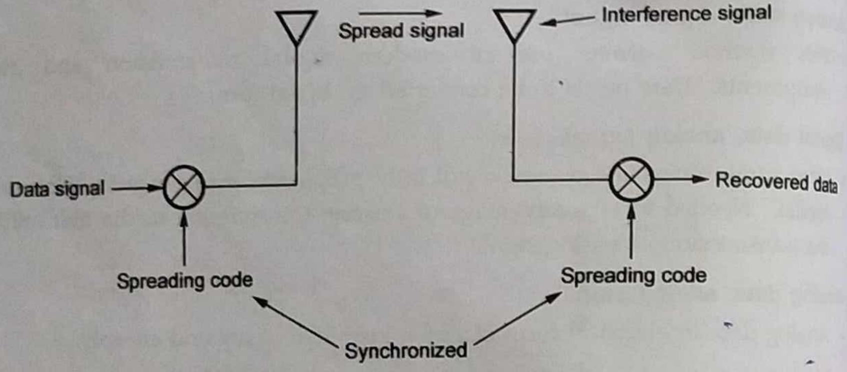


Fig. 2.8.1 Spread spectrum concept

- Spread Spectrum (SS) is apparent in the Shannon and Hartley channel-capa theorem.

2.8.1 Features of Spread Spectrum

- Following features of spread spectrum technology (whether DSSS or FHSS):
  1. Simplified multiple access : No requirement for coordination among users;
  2. Selective addressing capability if each station has a unique chip sequence-provides authentication : Alternatively, a common code may perform the CDMA function adequately since the probability of sta happening to be in synch is approximately 1/n;

3. Relative security from eavesdroppers : The low spread power and relatively fast direct sequence modulation by the pseudorandom code make detection difficult;
4. Interference rejection : The spread-spectrum receiver treats the other DSSS signals as thermal noise and suppresses narrowband interference.

2.8.2 Advantages of Spread Spectrum

1. Low power spectral density.
2. Privacy due to unknown random codes.
3. Random access possibilities.
4. Good anti-jam performance.
5. Reduced crosstalk interference.
6. Better voice quality/data integrity and less static noise.
7. Lowered susceptibility to multipath fading : Applying spread spectrum implies the reduction of multi-path effects.
8. Inherent security.
9. Co-existence.
10. Synchronization between stations in the system is not required (unlike TDMA, where synchronization is a critical feature of the system). This means that a station can access the system at any time.
11. Longer operating distances.
12. Hard to detect.
13. Hard to intercept or demodulate.

2.8.3 Direct Sequence Spread Spectrum (DS/SS)

- In SS system the signal spreading code is the so-called Pseudo-Noise (PN) sequence, which is generally periodic and consists of periodic coded sequence correlation properties.
- These signals are pseudorandom as they appear to be unpredictable to an outsider, though they can be generated by deterministic means by the person for whom they are intended.
- The polar signal c(t) representing this binary sequence is the pseudo-random carrier that is used to multiply the message signal m(t).
- Signal c(t) is a pseudorandom signal as it appears to be unpredictable though it can be generated by deterministic means (hence pseudorandom).

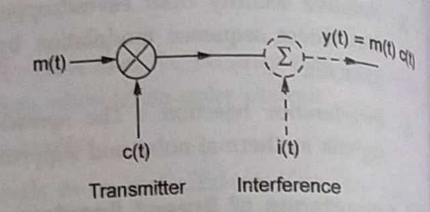


Fig. 2.8.2 DS/SS generator

Fig. 2.8.2 shows the generator of DS/SS signal.

- The bit rate of c(t) is much higher than the bit rate of m(t).

The basic pulse in c(t) is known as *chip* and the bit rate of c(t) is known as *chip rate* (R_c)

$$\text{Chip rate } R_c = \frac{1}{T_c}$$

where T_c is chip width.

- The autocorrelation function $\psi_c(t)$ of c(t) is very narrow.

Fig. 2.8.3 shows the signals at the SS generator.

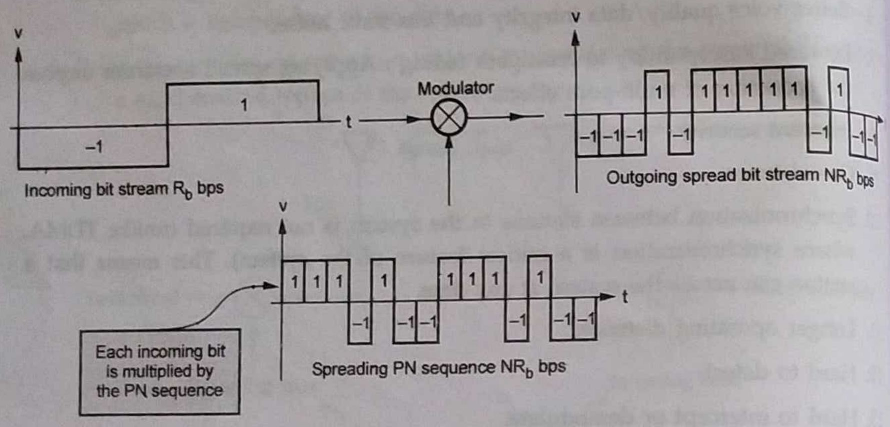

v
1
-1
t
Incoming bit stream R_b bps
Modulator
v
1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1 -1
Outgoing spread bit stream NR_b bps
v
1 1 1 1 1 1 1 1
-1 -1 -1 -1 -1 -1
t
Each incoming bit is multiplied by the PN sequence
Spreading PN sequence NR_b bps

Fig. 2.8.3 Principle of Direct Sequence Spread Spectrum

1) Detection

- At the receiver for detection a synchronous pseudorandom sequence c(t) similar t transmitter is used.

The received DS/SS signal y(t) is multiplied by c(t) to recover desired signal m(t).

$$\because \quad y(t)\, c(t) = m(t)\, c^2(t)$$

$$= m(t) \qquad \because c^2(t) = 1$$

Fig. 2.8.4 shows DS/SS receiver.

- A LPF is basically an integrator. The receiver performs the correlation incoming signal m(t) c(t) and locally generated c(t).

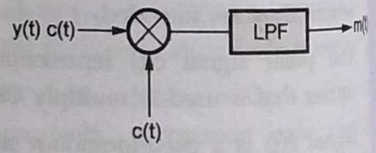


Fig. 2.8.4 DS/SS receiver

2) Signal Spectra

- Chip rate = R_c bits/sec and message symbol rate = R_b bits/sec.

The processing gain is given as

$$N = \frac{R_c}{R_b}$$

or

$$N = \frac{T_b}{T_c}$$

where T_c is chip width.

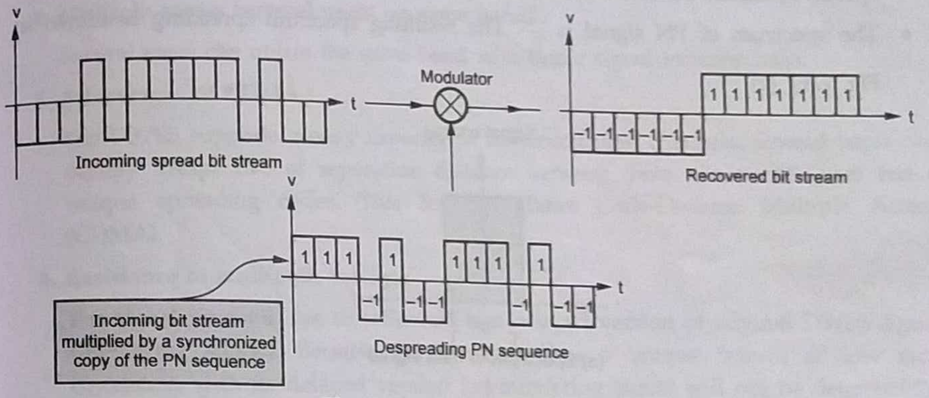


Fig. 2.8.5 De-spreading signal

- The Power Spectral Density (PSD) is given by

$$S_m(\omega) = T_b \operatorname{sinc}^2\left(\frac{\omega T_b}{2}\right) \qquad \text{For input signal (A)}$$

$$S_y(\omega) = T_c \operatorname{sinc}^2\left(\frac{\omega T_c}{2}\right) \qquad \text{For output signal (B)}$$

- The PSD of input signal m(t) and output signal of DS/SS y(t) is shown in the Fig. 2.8.6. Since the PSD bandwidth is directly proportional to bit rate, the PSD of y(t) is N times wider than PSD of m(t).

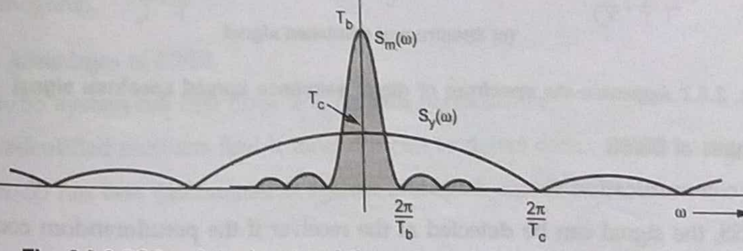


Fig. 2.8.6 PSDs of the input and the output signals of a DS/SS system

- The power of input and output equations are same. This indicates that PSD of y(t) is weaker than that of m(t) by a factor N (processing gain). In other words the spreading process reduces the PSD of a signal by factor N.

2.8.3.1 Approximate Pattern of DS/SS Signal

- Let the bit width of information signal is T, therefore data rate is $\frac{1}{T}$. The spectrum of signal, depending on encoding technique is approximately $\frac{1}{2T}$. Fig. 2.8.7 shows spread spectrum achieved by direct sequence technique.
- The spectrum of PN signal is $\frac{2}{T_c}$. The resulting spectrum spreading is shown in Fig. 2.8.7 (c)

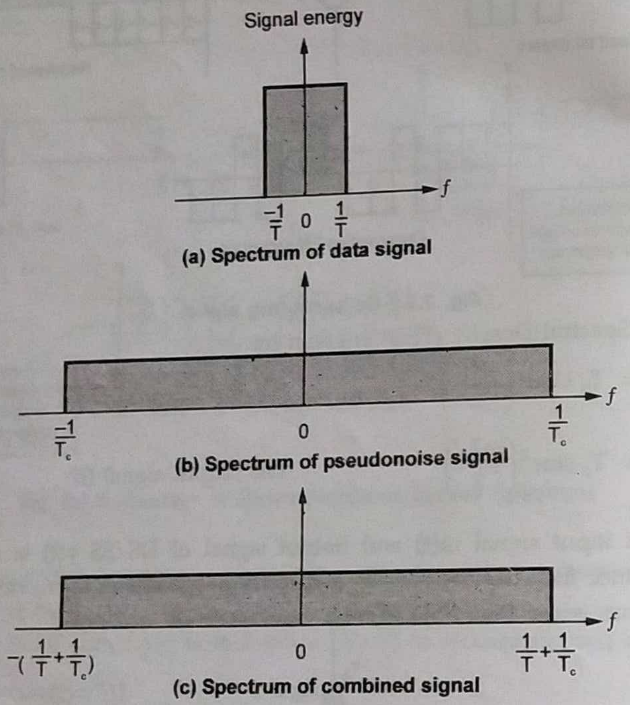


Fig. 2.8.7 Approximate spectrum of direct sequence spread spectrum signal

2.8.3.2 Features of DS/SS

1. **Secure communication :**

In DS/SS, the signal can be detected at the receiver if the pseudorandom code used at transmitter is known. This prevents unauthorized access of signal.

2. **Hiding of signal :**

The DS/SS signal spectrum is spread over a wide band, the signal PSD is very small. Hence it is easy to hide the signal within the noise floor.

3. **Jamming resistance :**

The DS/SS signal spectrum power is distributed over a wide band, hence these signals are difficult to jam. Because of spectral spreading PSD of jamming signal (interference) decreases by factor N.

While PSD of signal m(t) becomes stronger because of despreading.

4. **Multiple access (several users on same band) :**

Several users can utilize the same band with better signal to noise ratio.

5. **Advantages of CDMA :**

The DS/SS supports greater capacity of communication channels. Several users can occupy irrespective of separation distance between them. Since each user has a unique spreading codes. This features allows Code-Division Multiple Access (CDMA).

6. **Resistance to multipath fading :**

The signal received due to reflection is a delayed version of original DS/SS signal (interfering signal). Because DS/SS signal has a unique feature of low auto co-relation with its delayed version i.e. interfering signal will not be despread by c(t). Alternatively this minimizes the effect of multipath signals (multipath immunity).

7. **Near-far problem :**

The DS/SS suffers from the near-far problem. The near-far problem occurs because of unequal received power by the user.

When an unwanted signal strength is more because of its proximity of its transmitter to the receiver and the desired signal strength is weak. In such situation the desired signal may be suppressed. This problem can be eliminated by making all the codes orthogonal but it is difficult to make large number of codes orthogonal.

2.8.3.3 Advantages of DS/SS

1. DS/SS system has best noise and antijam performance.
2. Unidentified receivers find it most difficult to detect direct sequence signals.
3. DS/SS has best discrimination against multipath signals.

2.8.3.4 Disadvantages of DS/SS

1. DS/SS requires wideband channel with small phase distortion.
2. DS/SS has longer acquisition time.
3. The pseudo noise generator should generate sequence at high rates.

2.8.4 Frequency Hopping Spread Spectrum (FH/SS)

- In Frequency Hopping Spread Spectrum (FH/SS) scheme an FSK signal is generated then the frequency of FSK signal is shifted by pseudonoise (PN) sequence.

Fig. 2.8.8 shows FH/SS transmitter and receiver.

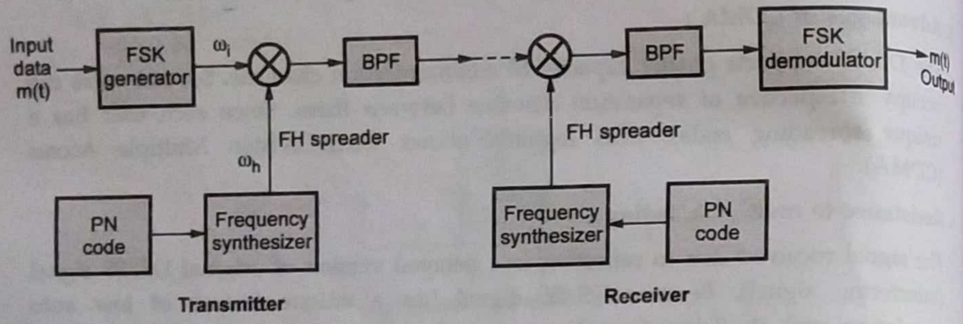


Fig. 2.8.8 FH/SS system

- The FSK output frequency is ω_i and synthesizer frequency is ω_h. The output of mixer contain $(\omega_h + \omega_i)$ and $(\omega_h - \omega_i)$. The BPF passes $(\omega_h + \omega_i)$ frequency components. The signal is now transmitted by pulses whose frequencies hop over a wide range of frequencies according to PN code. The BW of FH/SS signal is much more than FSK signal.
- The FH/SS receiver an identical PN code is synchronized with the received signal shifts the frequencies back to original FSK frequencies. These frequencies can be demodulated.
- There exists two conditions depending on frequency hopping rate R_h and symbol rate R_b.

i) When $R_h \le R_b$

the scheme is called as **Slow Frequency Hopping (SFH).**

ii) If $R_h > R_b$

the scheme is called as **Fast Frequency Hopping (FFH).**

2.8.4.1 Advantages of FH/SS

1. The systems bandwidth of FH/SS is very large.
2. It can be programmed to avoid some portions of spectrum.
3. It has relatively short acquisition time.
4. It has less distance effect.

Acquistion

Mobile computing and wireless communication

2.8.4.2 Disadvantages of FH/SS

1. FH/SS system requires complex frequency synthesizers.
2. ~~It is~~ not useful for range and range rate measurement.
3. ~~It~~ requires error correction.

2.8.4.3 Advantages of FH/SS over DS/SS

1. FH/SS can produce signals of much wider BW as compared to DS/SS.
2. The processing gain of FH/SS is much higher than DS/SS.
3. FH/SS is less susceptible to near-far problems than DS/SS.
4. Problems of relative power levels of co-channel signals are not critical in FH/SS as compared to DS/SS.

2.8.4.4 Comparison of DS/SS and FH/SS

Sr No.	Parameter	DS/SS	FH/SS
1.	Definition	PN sequence of large BW is multiplied with narrowband data signal.	Data bits are transmitted in different frequency slots which are changed by PN sequence.
2.	Signal spectrum	Data sequence is spread over entire BW of spread spectrum signal.	Data sequence is spread over small frequency slots of the spread spectrum signal.
3.	Chip rate R_c	Chip rate is fixed. It is rate at which PN sequence occurs $R_c = \frac{1}{T_c}$	Chip rate is maximum of hop rate or symbol rate $R_c = \max (R_h\ R_S)$
4.	Modulation technique	BPSK	M-ary FSK
5.	Processing gain	$PG = \frac{T_b}{T_c} = N$	$PG = 2^t$ t is bits in PN sequence
6.	Effect of distance	It is distance relative.	Effect of distance is less.
7.	Acquisition time	Long	Short

2.8.5 CDMA with DS/SS

- In CDMA with DS/SS, many users transmit their signals on the same channel bandwidth. Each transmitter receiver pair has a distinct pseudo-noise (PN) sequence. Thus signals of a particular transmitter are received by specified intended receiver only. Eventhough many users are transmitting simultaneously. This method is also called as Spread Spectrum Multiple Access (SSMA).
- The signals from others appear as additive interference which are rejected by spread spectrum decoder. The level of interference depends on number of transmitters at any time.
- The advantage of CDMA is that number of users sharing same channel can be increased or decreased very easily. Large number of users can transmit on the same channel if their messages are for short duration. It is desirable that PN sequences be mutually orthogonal.

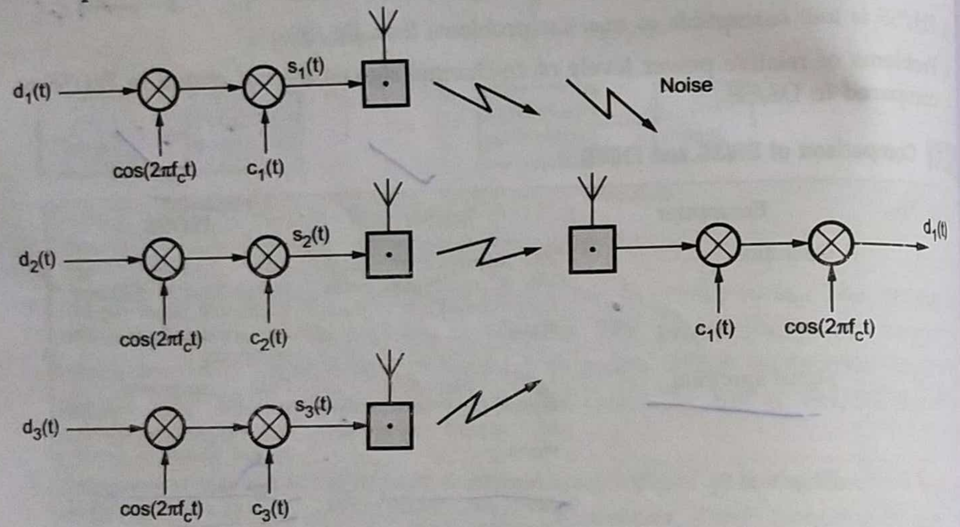


Fig. 2.8.9 CDMA with DS/SS system

2.8.6 CDMA with FH/SS

- In CDMA with FH/SS, the transmitter-receiver pair uses a distinct pseudo-random frequency hoping pattern. Therefore, the communication channel can be shared by multiple users simultaneously. The frequency hopping pattern for every transmitter-receiver pair is unique.
- The CDMA FH/SS systems can be used for mobile users. Because timing error does not affect this system, but it can affect DS/SS system.

- The frequency hopes over large bandwidth are possible compared to band spread obtained by DS/SS system. Therefore, processing gain is higher compared to DS/SS. Due to these facts the capacity of CDMA system using FH/SS is increased and hence more information rates are possible.

University Questions

1. *Define frequency hopping in spread spectrum ? Write note on TDMA, FDMA, CDMA.* **GTU : Winter 2011, Marks 7**
2. *What is direct sequence spread spectrum technology ? How does it works in CDMA technology ?* **GTU : Summer-13, Marks 7**
3. *What is DSSS ? Explain CDMA chip sequence with example.* **GTU : Winter 2013, Marks 7**
4. *Explain : Spread spectrum.* **GTU : Summer 2014, Marks 4**
5. *Explain in detail direct Sequence Spread Spectrum (DSSS).* **GTU : Winter 2014, Marks 7**
6. *Explain in detail Direct Sequence Spread Spectrum (DSSS).* **GTU : Summer - 2015, Marks 7**

2.9 Coding and Error Control

GTU : Summer-13

- In all data networks, there is a certain possibility that reception of a bit stream is altered by errors. Coding techniques aim to provide resistance to such errors by adding redundant bits to the transmitted bit stream so that the receiver can either detect and ask for a retransmission, or correct the faulty reception.
- Error correction is the process of detecting errors in transmitted messages and reconstructing the original error-free data. Error correction ensures that corrected and error-free messages are obtained at the receiver side.

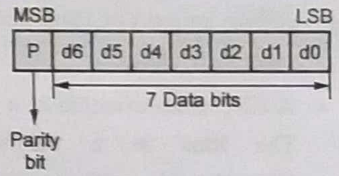


Fig. 2.9.1

- The process of adding this redundant information is known as channel coding, or Forward Error Correction (FEC). The error handling task is done by channel coding, before line coding.

2.9.1 Error Detection

2.9.1.1 Parity Check

- To detect and correct the errors, additional bits are added to the data bits at the time of transmission. The additional bits are called **parity bits**. The scheme is to append a parity bit to the end of a block of data. The data bits along with th parity bits form a **code word**

Parity Checking of Error Detection

- It is the simplest technique for detecting and correcting errors. The MSB of a 8-bits word is used as the parity bit and the remaining 7 bits are used as data message bits. The parity of 8-bits transmitted word can be either even parity o odd parity.

  Even parity : Even parity means the number of 1's in th given word including th parity bit should be even (2,4,6,....).

  Odd parity : Odd parity means the number of 1's in the given word including th parity bit should be odd (1,3,5,....).

2.9.1.2 Cyclic Redundancy Check

- Cyclic Redundancy-Check (CRC) codes are shortened binary cyclic codes that a widely used for error detection on digital communication links and data storage.
- A CRC is an example of a block code, but it can operate on blocks of any siz Given a message block of size k bits, it produces a compact digest of size r bi where r is a constant (typically between 8 and 32 bits in real implementations).
- Together, the k + r = n bits constitute a **code word**. Every valid code word has certain minimum Hamming distance from every other valid code word to aid i error detection.
- A CRC is an example of a polynomial code as well as an example of a cyclic cod The idea in a polynomial code is to represent every code wor $W = W_{n-1} W_{n-2} W_{n-3} \dots W_0$ as a polynomial of degree $n-1$. That is, we write

$$w(x) = \sum_{t=0}^{n-1} w_i x^i$$

- For example, the code word 11000101 may be represented as the polynomi $X^7 + X^6 + X^2 + 1$.
- The term code polynomial to refer to the polynomial corresponding to a cod word.
- The key idea in a CRC (and, indeed, in any cyclic code) is to ensure that eve valid code polynomial is a multiple of a generator polynomial, g(x).

Example 1 :

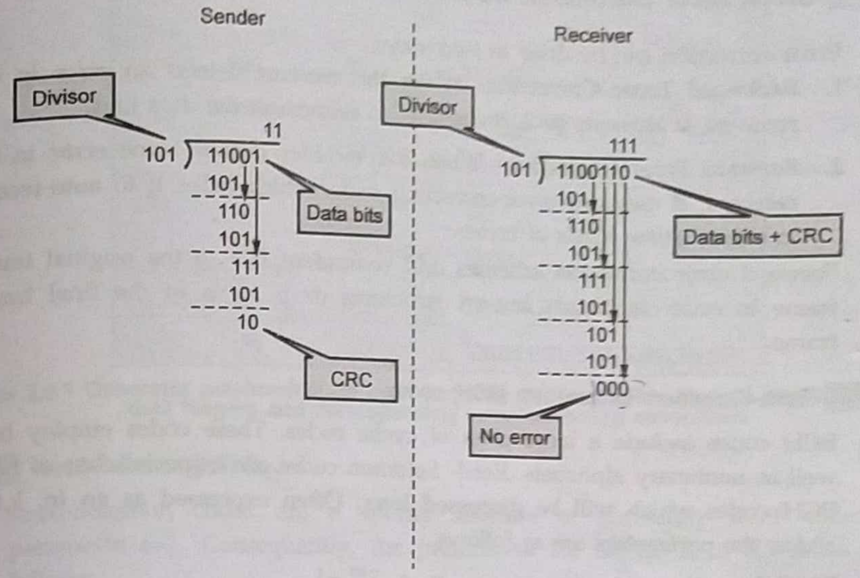


Fig. 2.9.2

Example 2.9.1 *Consider a (7, 4) cyclic code for encoding a data block m = [1010]. To find the generator polynomial g(x) for an (n, k) = (7, 4) code, we first factorize the polynomial $x^7 + 1$ and find the factor with degree n – k = 3 .*

Solution :

$$g(x) = (x^3 + x^2 + 1)$$

To encode the data block m = [1010], we multiply its

corrsponding polynomial m (x) = $x^2 + 1$ with g(x)

$$c(x) = m(x)\, g(x)$$
$$= (x^3 + x)(x^3 + x^2 + 1)$$
$$= x^6 + x^5 + x^4 + x$$

Thus the data block is encode to the codeword

$$c = [1110010]$$

2.9.2 Block Error Correction Codes

- Error correction can be done in two ways:
  1. **Backward Error Correction-** When the receiver detects an error in the d received, it requests back the sender to retransmit the data unit.
  2. **Forward Error Correction-** When the receiver detects some error in the d received, it executes error-correcting code, which helps it to auto-recover a to correct some kinds of errors.
- Forward error correction schemes add redundant b to the original transm frame in order to obtain known structures or p ns in the final transm frame.

2.9.2.1 Bose-Chaudhuri-Hocqueghem (BCH) codes

- BCH codes include a large class of cyclic codes. These codes employ binary well as nonbinary alphabets. Reed- Solomon codes are a special class of nonbin BCH codes which will be discussed later. Often expressed as an (n, k,t) b codes, the parameters are as follows.

Block loength : $n = 2^m - 1$

Number of check bits : $n - k \leq mt$

Minimum distance : $d_{min} \geq 2t + 1$

- These parameters provide larger selection of block lengths, code rates, and e correcting capabilities. Table 2.9.1 shows some examples of the parameten binary BCH code. Observed that for a given pair of (n, k) for block length gre 7, there are some flexibility for the parameter t. System designers can adjust th parameters to suit the system requirements.

n	k	t	g(x) (octal from)
7	4	1	13
15	11	1	23
	7	2	721
	5	3	2467
63	57	1	103
	51	2	12471
	45	3	1701317
	39	4	166623567
	36	5	1033500423
127	120	1	211
	113	2	41567
	106	3	11554743
	99	4	3447023271
	92	5	624730022327
255	247	1	435
	239	2	267543
	199	7	7633031270420722341
	179	10	22624710717340332416300455

Table 2.9.1 Generator polynomials (in octal form) for BCH codes for various block lengths, data lengths and corresponding error correcting capabilities

2.9.2.2 Reed-Solomon (RS) Codes

- Reed-Solomon codes are a special subclass of nonbinary BCH codes with parameter s=1. Consequently, the parameters for an (n, k, t) RS-codes are as follows.

Symbol length : m bits per symbol

Block length : $n = 2^m - 1$ symbols $= m(2^m - 1)$bits

Data length : k symbol

Size of check code : $n - k = 2t$ symbols $= m\ (2t)$ bits

Minimum distance : $d_{min} = 2t + 1$ symbols

- RS codes are known to have optimal distance properties.For fixed number of check bits, RS codes provide higher error correcting capability compared to other block codes.
- A property related to the extra redundancy provided by nonbinary alphabets, 2 information symbols can be added to the length n RS code (resulting in length n+2) without reducing the minimum distance of the code. These codes are known as extended-RS codes.
- RS codes are effective in correcting burst errors and excellent for application with large set of input symbols. One famous practical application of RS codes is the Compact Disc (CD) error control system

2.9.3 Convolutional Codes

- Convolutional codes offer an approach to error control coding substantially different from that of block codes.
- Convolutional encoders are encoders with memory. The outputs of the encoder not only depend on the current input bits but also certain amount of the previous bits.

Convolutional encoder :

- The convolutional encoder encodes the entire data stream, into a single codeword.
- It maps information to code bits sequentially by convolving a sequence of information bits with "generator" sequences.
- It does not need to segment the data stream into blocks of fixed size (Convolutional codes are often forced to block structure by periodic truncation).
- It is a machine with memory.
- This fundamental difference imparts a different nature to the design and evaluation of the code.
- Block codes are based on algebraic/combinatorial techniques.
- Convolutional codes are based on construction techniques. Easy implementation of convolutional encoder using a linear finite-state shift register.
- A convolutional code is defined by three parameters: n, k, and K with k inputs and n outputs.
- An (n, k, K) code processes input data k bits at a time and produces an output of n bits for each incoming k bits. So far this is the same as the block code. In practice, usually k=1 is chosen. Rc= k/n is the coding rate, determining the number of data bits per coded bit.
- K is the constraint length of the convolutional code (where the encoder has K-1 memory elements).

University Questions

1. *Explain the following in brief in context of GSM networks :*

   a) Mobile station b) BSS c) NSS d) OSS e) IMSI e) IMEI f) MSRN

   GTU : Summer-2013, Marks 7

2. *In GSM network, explain the role of network and switching subsystem.*

   GTU : Summer-2013, Marks 7

2.10 Automatic Repeat Request (ARQ)

- The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.
- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.
- **Error** control in the data link layer is based on automatic repeat request, which is the retransmission of data.
- ARQ is an error control (error correction) method that uses error-detection codes and positive and negative acknowledgments. When the transmitter either receives a negative acknowledgment or a timeout happens before acknowledgment is received, the ARQ makes the transmitter resend the message.
- The acknowledgement (ACK) or nonacknowledgement (NACK) messages, transmitted by the receiver to the transmitter to indicate a good (ACK) or a bad (NACK) reception of the previous frames.
- The ARQ is a MAC mechanism which is optional for implementation in the 802.16 standard. When implemented, the ARQ may be enabled on a per-connection basis. The perconnection ARQ is specified and negotiated during connection creation. A connection cannot have a mixture of ARQ and non-ARQ traffic.

2.11 Short Questions and Answers

Q.1 Define telecommunication traffic.

Ans. : In telecommunication system, traffic is defined as the occupancy of the server in the network. There are two types of traffic viz. voice traffic and data traffic. For voice traffic, the calling rate is defined as the number of calls per traffic path during the busy hour. In a day, the 60 minutes interval in which the traffic is highest is called Busy Hour (BH).

Q.2 What is multi-path fading ? Explain.

Ans. : In wireless communications, fading is the deviation of the signal attenuation affecting a certain propagation media. Discoloration may vary with time, the geographical position or frequency of the radio, which is often modeled as a random process. A fading channel is a communication channel experiencing fading. In wireless systems, fading can be due to multipath, called multi-path fading.

Q.3 What is spread spectrum technique ?

Ans. : Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is deliberately varied. This results in a much greater bandwidth than the signal would have, if its frequency were not varied. In other words, the transmitted signal bandwidth is greater than the minimal information

Notes

3 Multiple Access System, GSM, GPRS and Wireless Standards

Syllabus

Multiple access in Wireless System – *Multiple access scheme, frequency division multiple access, Time division multiple access, code division multiple access, space division multiple access, packet radio access, multiple access with collision avoidance.*

Global system for mobile communication - *Global system for mobile communication, GSM architecture, GSM entities, call routing in GSM,PLMN interface, GSM addresses and identifiers, network aspects in GSM,GSM frequency allocation, authentication and security*

General packet radio service(GPRS) - *GPRS and packet data network, GPRS network architecture, GPRS network operation, data services in GPRS, Applications of GPRS, Billing and charging in GPRS*

Wireless System Operations and standards - *Cordless Systems, Wireless Local Loop, WiMAX and IEEE 802.16 Broadband Wireless Access Standards, Mobile IP and Wireless Application Protocol*

Contents

3.1 Multiple Access in Wireless System

GTU : Summer-12, Winter-12

- Technique of sharing or dividing channel (transmission medium) among number of users is called as **multiple access technique.**
- All voice-oriented wireless networks such as cellular telephony or PCS use fixed assignment access.
- In fixed assignment access method, a fixed allocation of resource (frequency, time, code, etc.) are made available to user for communication purpose.
- Three basic fixed assignment multiple access techniques are :

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Code Division Multiple Access (CDMA)

- The choice of access method technology impacts on :

1. Capacity of channel
2. Quality of Service (QoS)

- Two basic techniques are used to differentiate between uplink and downlink transmissions are :

1. Frequency Division Duplexing (FDD)
2. Time Division Duplexing (TDD)

1.Frequency Division Duplexing (FDD)

- If forward (base station to mobile station-downlink) and reverse (Mobile station t base station-uplink) use different carrier frequencies that are sufficiently separated the duplexing system referred to as FDD.
- FDD is used for large coverage areas

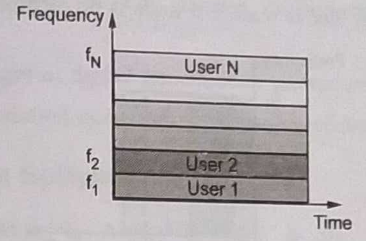
2.Time Division Duplexing (TDD)

- If both forward and reverse channels use the same frequency band fo communications but forward and reverse channels employ alternating time slots the duplexing system referred to as TDD.
- TDD can share one RF circuitry between forward and reverse channel. Th reciprocity of channels allow accurate open-loop power control (IS-95).
- TDD is preferred usually for low-power local communications.

3.1.1 Frequency Division Multiple Access (FDMA)

- In FDMA, all users are separated by their frequency of operation. All users m transmit simultaneously using a distinct carrier channel.

- A basic of Frequency Division Multiple Access (FDMA) is Frequency Division Multiplexing (FDM).
- A user is assigned a carrier f_i for each direction (uplink and downlink). A user may employ continuous transmission.
- Data (user's info) is modulated using the assigned carrier. Analog circuitry (VCO) is required to keep track of frequency shifts.



5-2

Fig. 3.1.1 FDMA

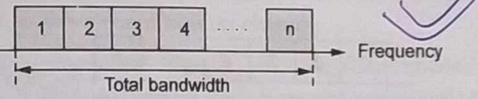


Fig. 3.1.2 FDMA bandwidth structure

Design Issues of FDMA system :

- Adjacent channel interference (specifically reverse channel).
- RF spectrum mask.
- Near-far problem is a concern specially on reverse link. Carriers belonging to one set are not adjacent.
- Guard bands - Reduces overall spectral efficiency.

3.1.1.1 Advantages of FDMA

1. Using well established technology.
2. No need for network timing.
3. No restriction regarding the type of baseband or the type of modulation.

3.1.1.2 Disadvantages of FDMA

1. Inter-modulation noise in the transponder leads to interference with other links-satellite capacity reduction.
2. Lack of flexibility in channel allocation.
3. Requires up-link power control to maintain quality.
4. Weak carrier tend to be suppressed.

3.1.2 Time-Division Multiple Access (TDMA)

- In TDMA system, a number of users share the same frequency band by ta assigned turns in using the channel.
- A base station controller assigns time slots to users and slot released upo completion of call.
- The entire band is used by the user during his slot. Fixed assignment e predetermined order. Slot is wasted if there is no information for transmissio

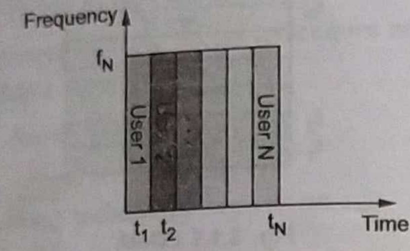


Fig. 3.1.3 TDMA

R4 d/a

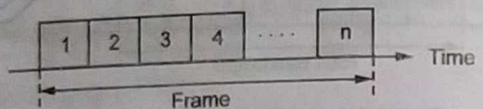


Fig. 3.1.4 TDMA frame structure

3.1.2.1 Advantages of TDMA

1. At a given time only one carrier is present on the channel hence intermodula distortion is eliminated.
2. TDMA transmission is separated in time domain. Processing of signal i domain is easier.
3. TDMA is most efficient method of transmission because of efficient u transmission resources.
4. TDMA can accomodate a wider range of bit rates by allowing a station t allocated several slots. Thus TDMA is more flexible than FDMA.
5. No intermodulation products (if the full transponder is occupied).
6. Saturated transponder operation possible.
7. With a flexible Burst Time Plan it will optimize capacity per connection.

3.1.2.2 Disadvantages of TDMA

1. Precise synchronization between stations is required. Transmission of every sta must occur during exact time slot.

2. Bit and frame timings must be maintained by TDMA.
3. Requires network-wide timing synchronization.
4. Analog signals must be converted to digital.
5. Interface with analog terrestrial plants is expensive.

3.1.2.3 Advantages of TDMA over FDMA

1. Digital equipment used in time division multiplexing is increasingly becoming cheaper.
2. There are advantages in digital transmission techniques. Example : Error correction.
3. Lack of inter-modulation noise means increased efficiency

3.1.3 Code Division Multiple Access (CDMA)

- Code Division Multiple Access (CDMA) is also called as spread spectrum communication. The term "spread spectrum" refers to the expansion of signal bandwidth, by several orders of magnitude in some cases, which occurs when a key is attached to the communication channel.
- In CDMA, the transmitted signals are not discriminated by their frequency assignment (as in FDMA), nor by their time slot assignment (as in TDMA), but by a characteristic code which is superposed on the information signal. This feature has allowed CDMA to gain attention in commercial satellite communication.
- CDMA was adopted in cellular mobile telephone as an interference-tolerant communication technology that increases capacity above analog systems.
- All concerned earth stations simultaneously share the same bandwidth and recognize the signals by various processes such as code identification.
- The two most common CDMA techniques are :
  1. Direct Sequence Spread Spectrum (DSSS), also called Pseudo-Noise (PN) modulation, which is the dominant technique.
  2. Frequency Hopping Spread Spectrum (FHSS)
- Spread Spectrum signals use fast codes that run many times the information bandwidth or data rate. These special "Spreading" codes are called "Pseudo Random" or "Pseudo Noise" codes. They are called "Pseudo" because they are not real Gaussian noise.

3.1.3.1 Functions of CDMA Receiver

- A typical CDMA receiver must carry out the following functions in order to acquire the signal, maintain synchronization, and reliably recover the data:

1. Synchronization with the incoming code through the technique of correlation detection;
2. De-spreading of the carrier;
3. Tracking the spreading signal to maintain synchronization;
4. Demodulation of the basic data stream;
5. Timing and bit detection;
6. Forward error correction to reduce the effective error rate;

- The first three functions are needed to extract the signal from the clutter of noise and other signals.
- The processes of demodulation, bit timing and detection, and FEC are standard for a digital receiver, regardless of the multiple access method.

3.1.3.2 Features of Spread Spectrum

- Following features of spread spectrum technology (whether DSSS or FHSS) :
  1. Simplified multiple access : No requirement for coordination among users;
  2. Selective addressing capability if each station has a unique chip code sequence-provides authentication : Alternatively, a common code may still perform the CDMA function adequately since the probability of stations happening to be in synch is approximately 1/n;
  3. Relative security from eavesdroppers : The low spread power and relatively fast direct sequence modulation by the pseudorandom code make detection difficult;
  4. Interference rejection : The spread-spectrum receiver treats the other DSSS signals as thermal noise and suppresses narrowband interference.

3.1.3.3 Advantages of Spread Spectrum

1. Low power spectral density.
2. Privacy due to unknown random codes.
3. Random access possibilities.
4. Good anti-jam performance.
5. Reduced crosstalk interference.
6. Better voice quality/data integrity and less static noise.
7. Lowered susceptibility to multipath fading : Applying spread spectrum implies the reduction of multi-path effects.
8. Inherent security.

9. Co-existence.
10. Synchronization between stations in the system is not required (unlike TDMA, where synchronization is a critical feature of the system). This means that a station can access the system at any time.
11. Longer operating distances.
12. Hard to detect.
13. Hard to intercept or demodulate.

3.1.4 Space Division Multiple Access (SDMA)

- In SDMA, there is control for radiated energy for each user which are served using spot beam antennas.
- Spot beams may use same frequency (as in TDMA or CDMA) or different frequencies (as in FDMA). Two types of antenna systems are employed.
  1. Sectorized antenna is one primitive form of SDMA.
  2. Adaptive antenna array uses steer multiple beams (one for each user). It is best suited for TDMA or CDMA systems.
- SDMA implementation is difficult for reverse link. It requires coordination of power levels. Also, huge power required to form beams.

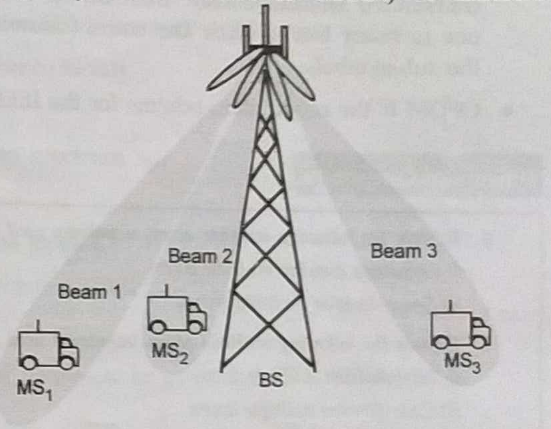


Fig. 3.1.5 Basic structure of SDMA system

3.1.5 Orthogonal Frequency Division Multiplexing (OFDM)

3.1.5.1 Problems Associated with TDMA, CDMA and FDMA

i) At high data rate, the symbol duration T_s becomes very small and the required system bandwidth becomes very large.

ii) If the symbol duration becomes vary small in TDMA, then the impulse response becomes very long. Hence computational effort increases.

iii) CDMA requires Rake receiver in addition to an equalizer.

iv) In FDMA, there is large spacing between carriers. This is wastage of precious spectrum.

OFDM overcomes above problems :

OFDM increases the symbol duration and all its carriers are mutually orthogonal. Above problems are almost removed by OFDM.

3.1.5.2 OFDM Functioning

- OFDM was chosen as modulation scheme to support high speed packet data transfer.
- OFDM is a form of multi carrier, multi symbol, multirate FDM in which user gets to use all the FDM channels together. It possesses the property of orthogonality.
- An OFDM modulation system uses several to many carriers that are all transmitted simultaneously. Each carrier transmits a sub-symbol that may encode one to many bits of data. The entire transmitted symbol consists of the sum of all the sub-symbols.
- OFDM is the modulation scheme for the IEEE 802.11 LAN wireless standard.

University Questions

1. *Explain the following multiple access techniques used to access the channel by mobile subscriber.*
   i) Frequency division multiple access
   ii) Space division multiple access. **GTU : Summer-12, Marks 7**
2. *Explain the following multiple access techniques used to access the channel by mobile subscriber.*
   i) Time division multiple access
   ii) Code division multiple access. **GTU : Summer-12, Marks 7**
3. *What is direct sequence spread spectrum technology ? Explain how it works in the CDMA technology ?* **GTU : Winter-12, Marks 7**

3.2 Global System for Mobile Communication (GSM)

GTU : Winter-11, 12, 13, 14, Summer-12, 14

- GSM technique is most widely used for digital cellular radio. A GSM system has maximum 200 full duplex channel per cell. Each channel has different uplink and downlink frequency. GSM handles channel access using a combination of slotted ALOHA, FDM and TDM.
- The Global System for Mobile (GSM) communications is a feature rich, digital wireless technology. GSM provides subscribers with high-quality digital wireless phone service and clarity, as well as enhanced call security and privacy.

- GSM is a second generation (2G) cellular system developed in Europe. It uses digital modulation and network level architectures and services. Commercial services of GSM was started in mid-1991.
- GSM can handle both voice and data traffic, the voice waveform being digitally encoded before transmission. GSM transmission is done within frequency bands of 900 MHz, 1800 MHz and 1900 MHz.

3.2.1 Basics of GSM

3.2.1.1 Features of GSM

1. Short message service allows to send and receive 126 character text messages.
2. Ability to use same phone in different networks.
3. Allows data transmission and reception across GSM networks at 9600 bps speed.
4. FAX transmission and reception across GSM networks at 9600 bps.
5. Call forwarding, call on hold, conference facility.
6. Rapid call setup.
7. More subscriber capacity in the given spectrum.
8. Smaller handsets.
9. Encrypted conversions that cannot be tapped.
10. Calling Number Identification Presentation (CLIP).
11. Real time call costs.
12. Closed User Group - Allows a set of phones to be classed as PBX extensions.

3.2.1.2 Services Provided by GSM

- Using ITU-T definitions, the telecommunication services of GSM can be divided into three categories

1. Bearer services or Data services 2. Teleservices 3. Supplementary services.

1. Bearer services or Data services

- A variety of data services can be offered by GSM.
  i) GSM users can send and receive data at rate upto 9600 bps.
  ii) Access to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks and Circuit Switched Networks using a variety of access methods and protocols such as x.25 and x.32.
- Since GSM is a digital network, a modem is not required between the users and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

iii) GSM supports Group 3 facsimile (FAX) service.

iv) Bidirectional SMS service, the messages are transported in a store-and-for fashion. SMS can be sent on point-to-point and cell broadcast mode (traffic news updates).

2. Teleservices

- The most basic teleservice supported by GSM is telephony. As with all communications, speech is digitally encoded and transmitted through the G network as a digital stream.
- There is also an emergency service, where the neai emergency-service pro is notified by dialling three digits (e.g. 911).
- GSM teleservice can also provide videotext, and teletext transmission.

3. Supplementary services

- Supplementary services are provided besides teleservices or bearer serv Supplementary services includes several forms of :

a) Number identification services

b) Call forwarding service c) Call completion services

d) Multiparty service e) Call restriction services.

3.2.1.3 GSM Radio Link Aspect

- GSM networks uses two 25 MHz bandwidth globally. This 25 MHz bandwid further divided into 124 carrier frequency channels each 200 kHz apart "Absolute Radio Frequency Channel Numbers (ARFCN)".

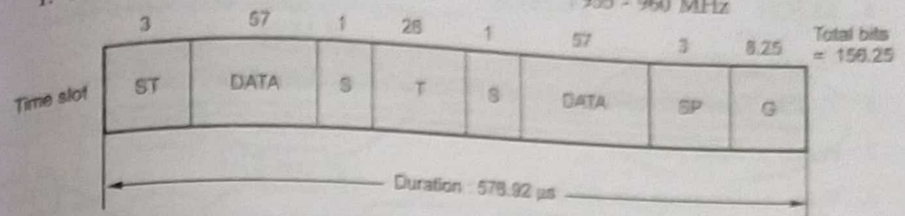
1. For subscriber to base transmission : 890-915 MHz (reverse link)

2. For base to subscriber transmission : 935-960 MHz (forward link)

- The ARFCN indicates a pair of channel (forward and reverse) which are sepa by 45 MHz. Each channel is time shared between 8 subscribers in TDMA sch with a frame duration of 4.615 ms. Radio transmissions on both forward reverse link are made at channel data rate of 270.833 kbps, using BT = 0.3 G modulation. Therefore, signalling bit period = 3.692 μs and effective da transmission rate per user is 33.854 kbps. But user data is sent at a maximum of 24.7 kbps because of GSM overload.
- Every Time Slot (TS) has 4156.25 bits, out of which 8.25 bits are used for g time and 6 bits are used for start and stop bits to prevent overlap with adj time slots. Each time slot has duration of 576.92 μs.

- The GSM air interface specifications are summarized as under.

1. Forward channel frequency : 935 - 960 MHz



ST : Start bits

S : Stealing bits

T : Training bits

SP : Stop bits

G : Guard bits

Fig. 3.2.1

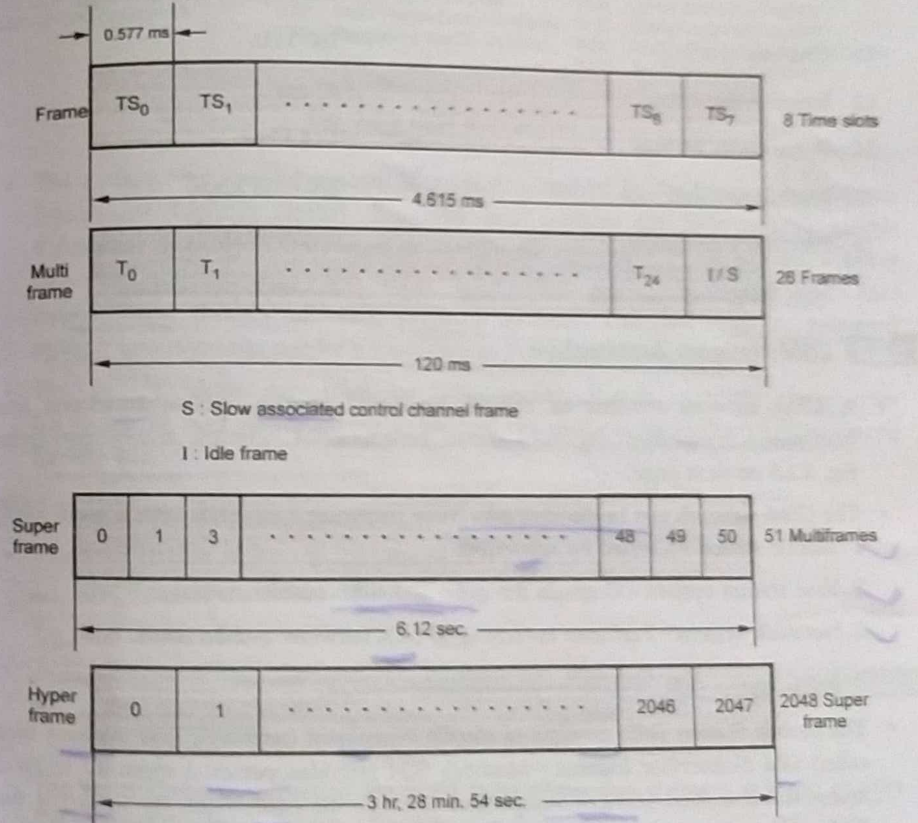


Fig. 3.2.2 GSM frame (Speech dedicated control channel frame)

2. Reverse channel frequency : 890 - 915 MHz

3. Forward and reverse channel bandwidth	: 25 MHz
4. ARFCN	: 0 to 124 and 975 to 1023
5. T_X / R_X frequency spacing	: 45 MHz
6. T_X / R_X Time slot spacing	: 3 Time slots
7. Frame / Burst period	: 4.615 ms
8. Voice transmission per RF channel	: 8
9. Time Slot (TS) period	: 576.9 µs
10. Bit period	: 3.692 µs
11. Modulation	: 0.3 GMSK (Gaussian Minimum Shift Keying)
12. Channel spacing	: 200 kHz
13. Interleaving delay	: 40 ms
14. Voice coder bit rate	: 13.4 kbps
15. Modulation data rate	: 270.8333 kbps
16. Frequency deviation	: 67.708 kHz
17. Slow frequency hopping	: 217 hops per second.

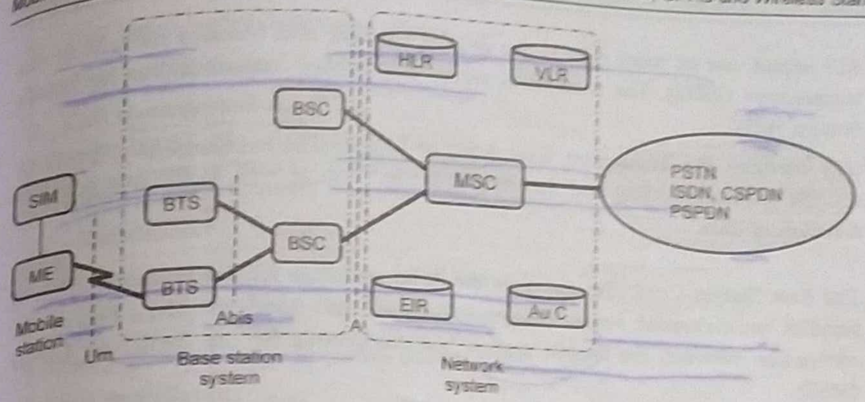
3.2.2 GSM Network Architecture

- A GSM network consists of several functional entities, whose functions and interfaces are specified. Fig. 3.2.3 shows generic GSM network architecture.(Refer Fig. 3.2.3 on next page)
- The GSM network can be divided into three parts.

1. Mobile station - Carried by subscriber
2. Base station system - Controls the radio link with mobile station
3. Network system - Performs switching of calls between mobile users.

3.2.2.1 Mobile Station (MS)

- The Mobile Station (MS) consists of mobile equipment (terminal) and a smart card called SIM (Subscriber Indentity Module). SIM provides personal mobility to have access to subscribed services irrespective of a specific equipment. By inserting the SIM card into another GSM equipment, the user can receive calls at that equipment, make calls from that equipment, and receive other subscribed servi



SIM : Subscriber Identity Module
ME : Mobile Equipment
BSC : Base Station Controller
BTS : Base Transreceiver controller
EIR : Equipment Identity Register
HLR : Home Location Register
VLR : Visitor Location Register
MSC : Mobile Service Switching Center
Au C : Authentication Center

Fig. 3.2.3 GSM architecture

- The mobile equipment (terminal) is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication and other information. The IMEI and IMSI are independent, thereby allowing personal mobility. The SIM may be protected against unauthorized use by a password or Personal Identity Number (PIN).
- The power levels supported by GSM mobile station currently range from 0.8 to 8.0 W, and power saving techniques are used on the air interface to extend battery life.

3.2.2.2 Base Station Subsystem (BSS)

- The base station subsystem consists of two parts -

1. Base Transceiver Station (BTS).
2. Base Station Controller (BSC).

- Abis interface allows the operation between BSC and BTS. The interface comprises traffic and control channels.

BTS

- The Base Transceiver Station has radio transceivers that define a cell and handles the radio-link protocols with Mobile Station (MS).

- BTS serves one or more cells in the cellular network and contains more than one transceivers (TRXs). The transceiver serves full duplex communication to Mobile Station (MS).
- BTS contains the Transcoder Rate Adapter Unit (TRAU). In TRAU, the GSM specific speech encoding and decoding is carried out, as well as the rate adaption function of data.

BSC

- The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping and handoffs. The BSC is the connection between the mobile station and the Mobile Service Switching Center (MSC).
- The functions of BSC and BTS are listed below.

Sr. No.	Base Station Controller (BSC)	Base Transceiver Station (BTS)
1.	Control of BTSs.	Interleaving and deinterleaving.
2.	Radio resource management.	Radio link protocols handling.
3.	Handoff management and control.	Full duplex communication to MS.

3.2.2.3 Network Switching System (NSS)

- The central component of network subsystem is the Mobile Services Switching Center (MSC). It acts as switching node of PSTN and provides the function needed to handle a mobile subscriber such as - Registration, authentication, location updating, handovers and call routing to roaming subscriber.
- Network subsystem includes data bases required for subscribers and mobile management. The Network subsystem also includes four different data bases -

1. Home Location Register (HLR) 2. Visitor Location Register (VLR)
3. Equipment Identity Register (EIR) 4. Authentication Center (AuC)

Mobile Switching Center (MSC)

- The MSC provides the connection to the fixed networks (PSTN or ISDN) with additional capabilities to support mobility management functions such as terminal registration location updating and handoff. These services are provided in conjunction with several functional entities which together form the network subsystem.
- The MSC does not contain mobile subscriber parameters. The major functions of MSC are listed below -

1. Call setup, supervision, and release.
2. Digit collection and translation.
3. Call routing /call handling.
4. Billing information collection.
5. Mobility management
   - Registration
   - Location updating
   - Call handoff between BSC and MSC
6. Management of radio resources during a call.
7. Echo cancellation.
8. Management of signalling protocol.
9. Interrogation of appropriate registers (VLR/HLR).

Home Location Register (HLR)

- The Home Location Register (HLR) and Visitor Location Register (VLR), together with MSC provide the call routing and roaming capabilities of GSM.
- The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with current location of Mobile Station (MS). The HLR database maintains unique International Mobile Subscriber Identity (IMSI) of each subscriber and VLR address. The location of the mobile station is typically in the form of the signalling address of the VLR associated with the mobile station.
- There is logically one HLR per GSM network, although it may be implemented as a distributed database.

HLR database can be grouped into two types :

1. Dynamic database

a. Location information for each subscriber.

2. Permanent database

a. International Mobile Subscriber Identity (IMSI)

b. Service subscription information.

c. Service restriction.

d. Supplementary services.

e. Mobile terminal characteristics.

f. Billing/accounting information.

Visitor Location Register (VLR)

- The Visitor Location Register (VLR) contains selected administrative informatio from HLR, necessary for call control and provision of subscribed services, for each mobile currently located in the geographical area controlled by the VLR.
- The VLR is a temporary database that stores the IMSI and customer informatio for each roaming subscriber who is visiting the coverage area of a particular MSC. There is one VLR part MSC. When a roaming mobile enters in MSC area, the MSC informs the associated VLR about the mobile and this information is registered.
- The VLR also contains information about the locally activated features such as call forward on busy. The temporary subscriber information in VLR includes -

1. International Mobile Subscriber Identity (IMSI and subscriber ID)
2. Features currently activated
3. Temporary Mobile Station Identity (TMSI)
4. Current location information about MS
5. Location where mobile is registered
6. Directory number to route calls to roaming station
7. Copy of subscriber data from HLR
8. Mobile station ISDN number
9. HLR address.

Equipment Identity Register (EIR)

- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved.
- The EIR data is in the form of white, grey and black lists which is consulted by network when it wishes to confirm the authenticity of terminal requesting servic Different list types and their contents are given below.

Sr. No.	Type	Meaning	Contents
1.	White list	Valid IMEI numbers	List of valid mobile equipments
2.	Grey list	IMEI under scanner	List of suspected mobile under observation.
3.	Black list	Prohibited IMEI numbers	List of mobile for which service is barred.

Authentication Center (AuC)

- The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.
- Authentication center maintains authentication keys and algorithms and provides security triplets (RAND, SRES, and K_c) to the VLR. This ensures, user authentication and radio channel encryption procedures to carryout within visited network.
- The AuC contains security modules for authentication keys (K_i), authentication algorithms (A_3) and cipher key generation algorithms (A_8).

Operation and Support Subsystem (OSS)

- The Operations and Support Subsystem (OSS) is the command center used to monitor and control the GSM system.
- The three areas of OSS are :

i) Network operations and maintenance.

ii) Subscription management (charging and billing etc.).

iii) Mobile equipment management.

- If an emergency occurs at a base station, the OSS can determine where the BTS is located, what type of failure occurred and what equipment the site engineer will need to repair the failure.

3.2.2.4 GSM Network Interfaces and Protocols

- Different types of interfaces are used in GSM systems for interconnecting its subsystems.

1. U_m interface 2. Abis interface 3. A interface

U_m interface :

- The U_m interface is radio or air interface. The U_m radio interface is used to communicate between Mobile Station (MS) with Base Transceiver Station (BTS).

Abis interface :

- The Abis interface is used for inter communication between BSC and BTS. This interface is defined by GSM equipment manufacturer. It carries traffic and control channel data.

A interface :

- The A interface allows the interconnection between BSC and MSC. These are physically connected by dedicated/leased lines or microwave links. The physical layer of A interface is a 2 Mbps CCITT digital connection.

- The A interface allows a service provider to use base stations and switchi equipment made by different manufacturers.

B interface :

- The B interface exists between the MSC and the VLR. It uses a protocol known a the MAP/B protocol. As most VLRs are collocated with an MSC, this makes th interface purely an "internal" interface.
- The interface is used whenever the MSC needs access to data regarding a M located in its area.

C interface :

- The C interface is located between the HLR and a GMSC or a SMS-G. When a cal originates from outside the network, i.e. from the PSTN or another mobil network it has to pass through the gateway so that routing information require to complete the call may be gained.
- The protocol used for communication is MAP/C, the letter "C" indicating that th protocol is used for the "C" interface. In addition to this, the MSC may optionall forward billing information to the HLR after the call is completed and clear down.

D interface :

- The D interface is situated between the VLR and HLR. It uses the MAP/ protocol to exchange the data related to the location of the ME and to th management of the subscriber.

E interface :

- The E interface provides communication between two MSCs. The E interfa exchanges data related to handover between the anchor and relay MSCs using th MAP/E protocol.

F interface :

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

G interface :

- The G interface interconnects two VLRs of different MSCs and uses the MAP/ protocol to transfer subscriber information, during e.g. a location upd procedure.

H interface

- The H interface exists between the MSC the SMS-G. It transfers short messag and uses the MAP/H protocol.

I interface :

- The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through the BSS.
- Various GSM interface standards are shown in Fig. 3.2.4.

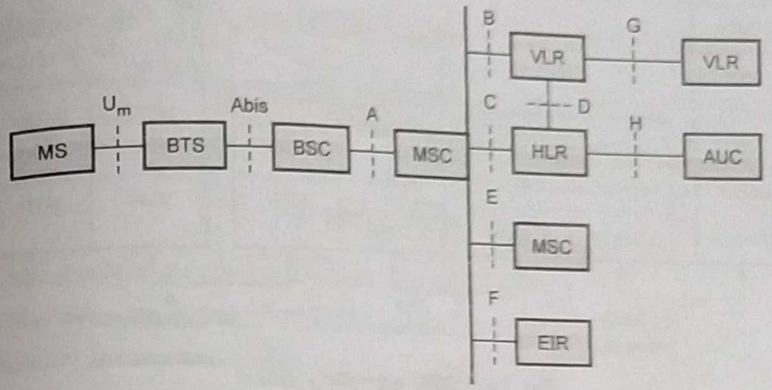


Fig. 3.2.4 GSM Interface

3.2.3 GSM Signaling Protocol Architecture

- The MS communicates with MSC for providing system connection, mobility and radio resource management.

Layered structure/OSI model : The OSI model views the communications between user application processes as being partitioned into self-contained layers that contain tasks that can be implemented independently of tasks in other layers. A message sent between two network nodes travels downward in the protocol stack of the sending node. As the message propagates through the layer information is added to the original message at each layer. After transmission to the receiving network node, the message propogates upward through the receiving node protocol stack.

- Signaling model for GSM system is shown in Fig. 3.2.5.
- The signalling model shows various protocols used between the different GSM interfaces and at the OSI levels. The MSC communicates with the various networks connected to PSTN using various protocols.
- The GSM signaling protocol stack consists of three layers.

1. Physical layer (Layer - 1)
2. Data link layer (Layer - 2)
3. Network or Messaging layer (Layer - 3)

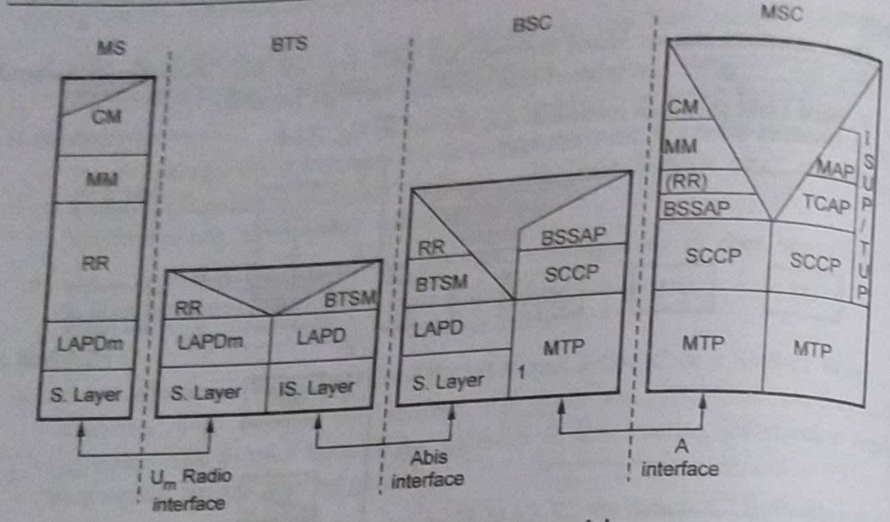


Fig. 3.2.5 GSM signalling model

3.2.3.1 Physical Layer (Layer-1)

- Physical layer is defined for U_m air interface. The physical layer specifies :

a) how the information from different voice and data are formatted in packets.

b) radio modem description.

c) varify of services.

d) modulation and control techniques.

e) power control methodology.

f) time synchronization.

3.2.3.2 Data Link Layer (Layer-2)

- Signaling and control data is communicated by layer-2 and layer-3 messages.
- The data link layer check the flow of data packets to layer-3.
- The data link control protocol is known as $LAPD_m$, where m indicates modified version of LAPD.

184 bits

Address (8 - bits)	Control (8 - bits)	Length-Indicator (8 - bits)	Information (variable)	Fill-in (variable)

Fig. 3.2.6 Frame format of of $LAPD_m$

3.2.3.3 Networking or Messaging Layer

- The networking or messaging layer is responsible for protocols to establish, maintain and terminate a mobile communication session.
- This layer specifies the messages on logical channels encapsulated in DLL frames.

Transaction identifier	Protocol discriminator	Message type	Information	Information identifier

Fig. 3.2.7 Message format

- GSM standard divides the messages into sublayers as -

a) Radio Resource Management (RRM)

b) Mobility Management (MM)

c) Communication Management (CM)

3.2.4 Identifiers in GSM System

- The MIN (Mobile Identification Number) is a number that uniquely identifies a mobile telephone subscriber. GSM uses a number of descriptors to identify subscribers, equipment, and fixed stations/areas. Many are temporary and used to maintain the confidentiality of fixed identities.
- There are basically three numbers that identify the mobile subscriber; these are IMSI, MS-ISDN, and the TMSI, which is a temporary identification number that is assigned by the serving MSC/VLR combination.
- The TMSI is mainly used for security reasons to avoid broadcasting the IMSI over the RF air interface, thereby making it harder for eavesdroppers. The TMSI is supposed to be changed on a per-call basis as recommended by GSM specific actions.

Subscriber Device Identification

- The mobile Subscriber Device (SD) can have different identification system depends on the type of networks such as TDMA, CDMA and GSM.

- The TMSI is mainly used for security reasons to avoid broadcasting the IMSI over the RF air interface, thereby making it harder for eavesdroppers. The TMSI is supposed to be changed on a per-call basis as recommended by GSM specific actions.

Subscriber Device Identification

- The mobile Subscriber Device (SD) can have different identification system depends on the type of networks such as TDMA, CDMA and GSM.

3.2.4.1 Mobile Station ISDN Identification (MSISDN)

- The MSISDN is a number which uniquely identifies a mobile telephone subscription in the public switched telephone network numbering plan. According to the CCITT recommendations, the mobile telephone number or catalogue number to be dialled is composed in the following way :
- MSISDN composed of :

MSISDN = CC + NDC + SN

CC = Country Code

NDC = National Destination Code

SN = Subscriber Number

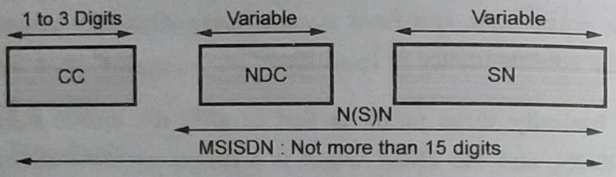


Fig. 3.2.8 MSISDN number

- CC (Country Code) is the country in which the VLR mobile station is registered.
- A National Destination Code (NDC) is allocated to each GSM PLMN. In some countries, more than one NDC may be required for each GSM PLMN. The international MSISDN number may be of variable length. The maximum length shall be 15 digits, prefixes not included.
- SN - is Subscriber Number
- N(S) N - National (Significant) Number consists of NDC and SN.
- The length of the MSISDN depends on the structure and numbering plan of each operator, as an application of CCITT recommendation E.164.

3.2.4.2 International Mobile Subscriber Identity (IMSI)

- The IMSI is the information which uniquely identifies a subscriber in a GSM/PLMN. An IMSI is assigned to each authorized GSM user. It consists of a Mobile Country Code (MCC), Mobile Network Code (MNC) and a PLMN unique Mobile Subscriber Identification Number (MSIN). The IMSI is not hardware-specific. Instead, it is maintained on a SC by an authorized subscriber and is the only absolute identity that a subscriber has within the GSM system.
- For a correct identification over the radio path and through the GSM PLMN network, a specific identity is allocated to each subscriber. This identity is called the International Mobile Subscriber Identity (IMSI) and is used for all signalling in the PLMN. It will be stored in the Subscriber Identity Module (SIM), as well as in the Home Location Register (HLR) and in the serving Visitor Location Register (VLR).
- According to the GSM recommendations, the IMSI will have a length of maximum 15 digits. All network-related subscriber information is connected to the IMSI.
- The IMSI consists of three different parts :

IMSI = MCC + MNC + MSIN

MCC = Mobile Country Code (3 digits)

MNC = Mobile Network Code (2 digits)

MSIN = Mobile Subscriber Identification Number (max 10 digits)

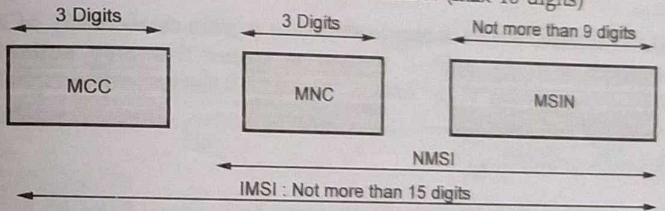


Fig. 3.2.9 IMSI number

- Mobile Country Codes (MCC) are used to identify mobile stations in wireless telephone networks.
- Mobile Network Code (MNC) uniquely identifies the home GSM PLMN of the mobile subscriber. It consists of 3 digits.
- Mobile Station Identification Number (MSIN) uniquely identifies the mobile subscriber within a GSM PLMN. The first 3 digits identify the logical HLR-ID of the mobile subscriber.
- National Mobile Station Identity (NMSI) consists of the MNC followed by the MSIN and is to be assigned by individual administration.

3.2.4.3 Temporary Mobile Subscriber Identity (TMSI)

- The TMSI is a temporary number used instead of IMSI to identify an MS. The TMSI is used for the subscriber's confidentiality on the air interface.
- The TMSI has only local significance (that is, within the MSC/VLR area) and is changed at certain events or time intervals.

3.2.4.4 Mobile Station Roaming Number (MSRN)

- A MSRN is used during the call setup phase for mobile terminating calls. Each mobile terminating call enters the GMSC in the PLMN. The call is then re-routed by the GMSC, to the MSC where the called mobile subscriber is located. For this purpose MSRN is allocated by the MSC and provided to the GMSC.
- The MSRN consists of -

a. Country Code (CC)

b. National Destination Code (NDC)

c. Subscriber Number (SN)

MSRN = CC + NDC + SN

3.2.4.5 International Mobile Station Equipment Identity (IMEI)

- The IMEI is used for equipment identification. The IMEI is the unique identity of the equipment used by a subscriber by each PLMN and is used to determine authorized (white), unauthorized (black) and malfunctioning (gray) GSM hardware.
- An IMEI uniquely identifies a mobile station as a piece or assembly of equipment. In conjunction with the IMSI, it is used to ensure that only authorized users should be granted access to the system. An IMEI is never sent in cipher mode by a MS.

IMEI = TAC + FAC + SNR + sp

TAC = Type Approval Code (6 digits), determined by a central GSM body

FAC = Final Assembly Code (2 digits), identifies the manufacturer.

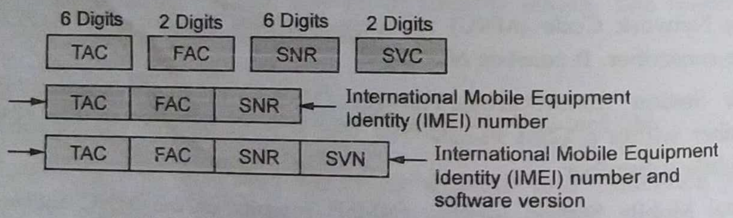

6 Digits
2 Digits
6 Digits
2 Digits
TAC
FAC
SNR
SVC
TAC
FAC
SNR
International Mobile Equipment Identity (IMEI) number
TAC
FAC
SNR
SVN
International Mobile Equipment Identity (IMEI) number and software version

Fig. 3.2.10 Formation of IMEI number

SNR = Serial Number (6 digits), an individual serial number of six digits uniquely identifying all equipment within each TAC and FAC.

sp = Spare for future use (1 digit)

According to the GSM specification, IMEI has the length of 15 digits.

3.2.4.6 Location Area Identity (LAI)

- LAI is used for location updating of mobile subscribers.

LAI = MCC + MNC + LAC

- MCC is Mobile Country Code (3 digits), identifies the country. It follows the same numbering plan as MCC in IMSI.
- MNC is Mobile Network Code (2 digits), identifies the GSM/PLMN in that country and follows the same numbering plan as the MNC in IMSI.
- LAC is Location Area Code, identifies a location area within a GSM PLMN network. The maximum length of LAC is 16 bits, enabling 65, 536 different location areas to be defined in one GSM PLMN.

3.2.4.7 Cell Global Identity (CGI)

- CGI is used for cell identification within the GSM network. This is done by adding a Cell Identity (CI) to the location area identity.

CGI = MCC + MNC + LAC + CI

- CI is Cell Identity, identifies a cell within a location area, maximum 16 bits

3.2.4.8 Base Station Identity Code (BSIC)

- BSIC allows a mobile station to distinguish between different neighbouring base stations.

BSIC = NCC + BCC

- NCC is Network Colour Code (3 bits), identifies the GSM PLMN. It does not uniquely identify the operator. NCC is primarily used to distinguish between operators on each side of border.
- BCC is Base Station Colour Code (3 bits), identifies the Base Station to help distinguish between BTS using the same BCCH frequencies.
- **Radio Base Station Identity Code (RBSIC)** - Used by the mobile operator to identify the RBS's within a wireless network.

3.2.4.9 Location Number (LN)

- Location number is a number related to a certain geographical area, as specified by the network operator by "tying" the location numbers to cells, location areas or MSC/VLR service areas.
- The location number is used to implement features like regional/local subscription and geographical differentiated charging.

3.2.4.10 Global Title (GT) and Global Title Translation (GTT)

- The GT is an address of fixed network element. The (is used for the addressing of network nodes such as MSCs, HLRs, VLRs, AUCs d EIRs in accordance with E.164.
- The GTL is performed by SCCP translation function to provide the correct signalling point address information for the subsequent routing of the message to correct network node.

3.2.5 GSM Channel

- The GSM cellular system is based on the use of time division multiple access to provide additional user capacity over a limited amount of radio frequency spectrum.
- A single GSM RF carrier can support up to eight MS subscribers simultaneously. Each channel occupies the carrier for one eighth of the time. This technique is called Time Division Multiple Access (TDMA).
- Time is divided into discrete periods called timeslots. The timeslots are arranged in sequence and are conventionally numbered 0 to 7. Each repetition of this sequence is called a TDMA frame. Each MS telephone call occupies one timeslot (0 to 7) within the frame until the call is terminated, or a handover occurs. The TDMA frames are then built into further frame structures according to the type of channel.

  Frames - GSM system divides the radio link connection time into eight equal and repeating timeslots known as frames.

  Multi-frames - The system can use several different types of repeating frame structures known as multi- frames.
- For a system to work correctly, the timing of the transmissions to and from the MS is critical. The MS or BS must transmit the information related to one call at exactly the right moment, or the timeslot will be missed. The information carried in one timeslot is called a burst.

- Each data burst, occupying its allocated timeslot within successive TDMA frames, provides a single GSM physical channel carrying a varying number of logical channels between the MS and BTS.
- Fig. 3.2.11 shows TDMA time frame structure

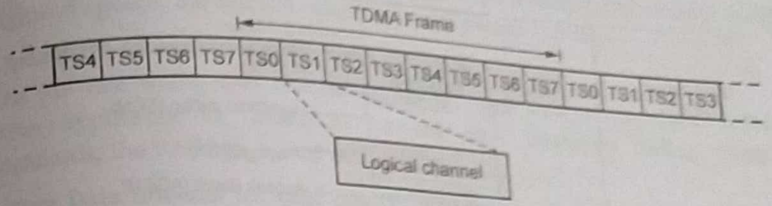


Fig. 3.2.11 TDMA time frame structure

3.2.6 Logical Channels

- There are two basic types of logical channels in GSM :

1. Traffic Channels (TCH)
2. Control Channels (CCH)

- Traffic Channels (TCH) are used to carry either digitally encoded user speech or user data in uplink and downlink directions. Initial GSM specification specifies full rate speech channels (22.8 kB/s) and data channels (9.6, 4.8 and 2.4 kB/s) are defined as TCH.
- Control Channels (CCH) carry signalling and synchronizing commands between the base station and mobile station. Three basic types of Control Channels (CCH) are :

  i) Broadcast Control Channels (BCCH) ii) Common Control Channels (CCCH)

  iii) Dedicated Control Channels (DCCH)
- Each control channel is further subdivided. Fig. 3.2.12 shows different subcategories of traffic and control channels in GSM. (Refer Fig. 3.2.12 on next page)

3.2.6.1 Traffic Channels (TCH)

- Traffic Channels (TCH) carry encoded speech and data. A TCH is a group of 26 TDMA frames, called multiframe. Each TDMA frame is having 120 ms duration. Out of 26 TDMA frames, 24 are used as TCH frames, one frame (13^{th}) is for SACCH and one frame (26^{th}) is unused or idle frame.
- The TCH supports two information rates :

  1. Full rate (TCH/F) . 2. Half rate (TCH/H).

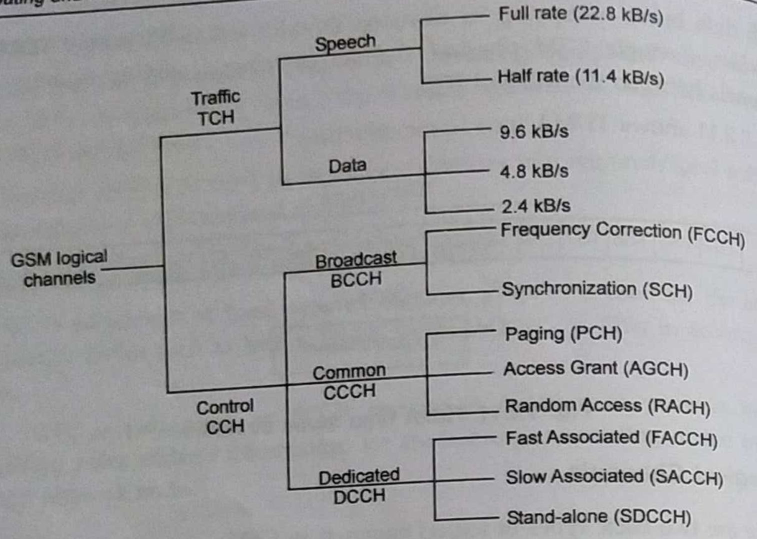


Fig. 3.2.12 GSM channel structures

- When transmitted as full rate, the user data is occupied within one TS per frame. When transmitted as half rate, the user data is occupied into the same time slot but is sent in alternate frames.
- The 26th frame contains idle bits if full rate TCHs are used and contains SACCH data if half rate TCHs are used.

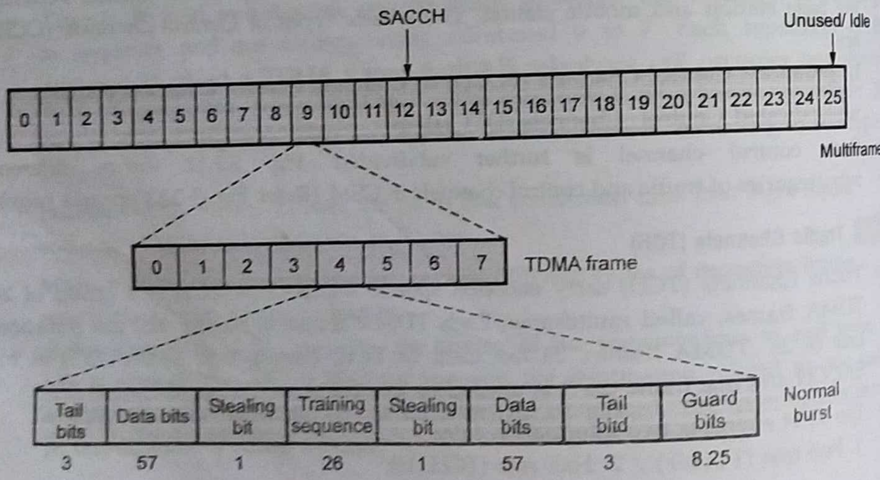


Fig. 3.2.13

Full Rate TCH

- Different full rate TCH for speech and data channels are as mentioned subsequently.

1. Full Rate Speech Channel (TCH/FS) :

- The full rate speech is digitized at 13 kbps. After adding GSM channel coding to digitized speech, the full rate speech channel carries 22.8 kbps.

2. Full Rate Data Channel for 9600 bps (TCH/F9.6) :

- The full rate traffic data channel carries raw user data which is sent at 9.6 kbps. After application of additional forward error correction coding using GSM standards, the 9.6 kbps is sent at 22.8 kbps.

3. Full Rate Data Channel for 4800 bps (TCH/F4.8) :

- The full rate traffic data channel carries raw user data, which is sent at 4.8 kbps. With application of additional forward error correction coding using GSM standards, the 4.8 kbps data is sent at 22.8 kbps.

4. Full Rate Data Channel for 2400 bps (TCH/F2.4) :

- The full rate traffic data channel carries raw data, which is sent at 2.4 kbps. With application of additional forward error correction coding using GSM standards, the 2.4 kbps data is sent at 22.8 kbps.

Half Rate TCH

- Different half rate TCH for speech and data channels are as mentioned :

1. Half Rate Speech Channel (TCH/HS) :

- The half rate speech channel can carry digitized speech which is sampled at a rate half that of a full rate channel. GSM anticipate the availability of speech coders can digitize speech at about 6.5 kbps. After adding GSM channel coding to the digitized speech, the half rate speech channel will carry 11.4 kbps.

2. Half Rate Data Channel for 4800 bps (TCH/H4.8)

- The half rate traffic data channel carries raw user data which is sent at 4800 bps. After application of forward error correction using GSM standards, the 4800 bps data is sent at 11.4 kbps.

3. Half Rate Data Channel for 2400 bps (TCH/H2.4)

- The half rate traffic data channel carries raw user data which is sent at 2400 bps. After application of additional forward error correction using GSM standards, the 2400 bps data is sent at 11.4 kbps.

3.2.6.2 Control Channels (CCH)

- Control Channels (CCH) are used, when mobile is idle or in dedicated mode. In idle mode, CCH exchange the signalling information needed to change dedicated mode.
- The three basic control channels are : Broadcast (BCCH), Common (CCCH) and Dedicated (DCCH). Each control channel consists of several logical channels which are distributed in time to provide necessary GSM control functions.

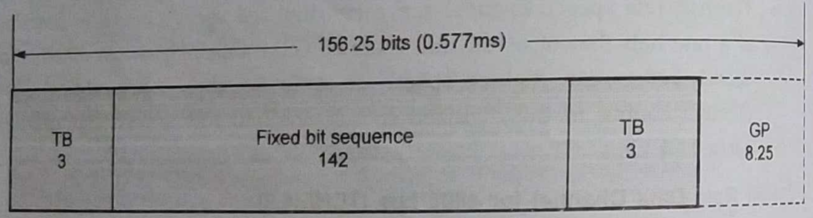
Broadcast Control Channel (BCCH)

- The Broadcast Control Channel (BCCH) is a unidirectional base to mobile channel which provides general information about the network, the cell in which the mobile is currently located and adjacent cells.
- The BCCH includes two channels :

1. Frequency Correction Channel (FCCH) 2. Synchronization Channel (SCH)

1. Frequency Correction Channel (FCCH) :

- FCCH is a base to mobile channel which provides information for carrier synchronization. The FCCH is a special data burst which occupies TS0 slot for the very first GSM frame (frame 0) and is repeated every ten frames within a control channel multiframe. The FCCH allows Mobile Subscriber (MS) to synchronize its internal frequency standard (local oscillator) with the frequency of Base Station (BS). In its first burst of FCCH, all zero bits are sent to indicate unmodulated carrier. Fig. 3.2.14 (a) shows Frequency Correction Burst (FCCH) structure.



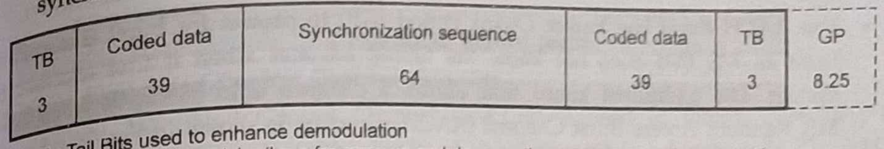
TB : Tail Bits used to enhance demodulation
GP : Guard period, which allows for ramp up and down as the power is turned on and off.

Fig. 3.2.14 (a) Frequency correction burst

2. Synchronization Channel (SCH) :

- The Synchronization Channel (SCH) is a base to mobile channel which carries information for frame synchronization and identification of the Base Station (BS) transceiver. It also contains BSIC (Base Station Identity Code) and the frame number in relation to the hyperframe.

- In the frame following the FCCH, the BTS transmits with SCH in time slot 0. The SCH has a unique burst structure as well. It contains 64-bit binary (training) sequence that is same throughout all GSM networks and known to the MS. The BSIC is assigned to each BTS in GSM system. The SCH is transmitted once every ten frames within the control channel multiframe. Fig. 3.2.14 (b) shows synchronization burst structure.



TB : Tail Bits used to enhance demodulation
GP : Guard period, which allows for ramp up and down as the power is turned on and off.
Synchronization Sequence : Used for adaptive equalization and BTS identification
Coded Data : Encrypted user data or signalling control information.

Fig. 3.2.14 (b)

Common Control Channels (CCCH)

- The Common Control Channel (CCCH) includes : three different types of channels.

1. Paging Channel (PCH) ; which is a forward link channel.
2. Access Grant Channel (AGCH); which is a forward link channel.
3. Random Access Channel (RACH); which is a reverse link channel.

1. Paging Channel (PCH) :

- The Paging Channel (PCH) is a part of CCCH and is a base to Mobile (forward link) channel used to alert a mobile to a call originating from the network.
- The PCH generates paging signals from the base station to all Mobile Subscribers (MSs) in the cell and registers incoming call. The paging is done by transmitting IMSI of target subscriber along with request for acknowledgement on RACH.

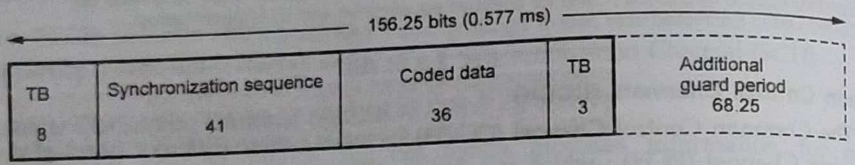
2. Access Grant Channel (AGCH) :

- The Access Grant Channel (AGCH) is part of CCCH and is a base to mobile (Forward link) channel used to assign dedicated resources, such as Stand-alone Dedicated Control Channel (SDCCH) or Traffic Channel (TCH) to a mobile which has previously requested through RACH.
- AGCH is used to direct a mobile station to another type of control channel i.e. SDCCH or TCH, in order to complete the process of setting up a call and/or transferring information.

3. Random Access Channel (RACH)

- The Random Access Channel (RACH) is the reverse (mobile to base) channel. With the help of RACH, Mobile Station (MS) originates a call, sends signalling messages when not on call, acknowledges message from the BTS.

- The RACH uses the slotted ALOHA access scheme i.e. all mobiles requests access or respond to PCH alert within TS0 of a GSM frame. At BTS every frame will accept RACH transmissions from Mobile Station (MS). If RACH has been received successfully by the BTS, the network will direct the mobile station to the SDCCH-a two-way control channel designated just for this type of communication between mobile station and the network. Actually RACH carries very little information.
- The RACH burst has longer Guard Period (GP) to protect for burst transmission from an MS that does not know the timing advance when it first accesses the system. The additional guard time allows a distance upto 35 km between BS to MS. Random Access Burst Channel (RACH) structure is shown in Fig. 3.2.15.



TB	Synchronization sequence	Coded data	TB	Additional guard period
8	41	36	3	68.25

TB : Tail bits use l to enhance demodulation
Synchronization Sequence : Used for adaptive equalization and BTS identification
Coded data : Encrypted user data or signalling control information
GP : guard period

Fig. 3.2.15 Random access burst

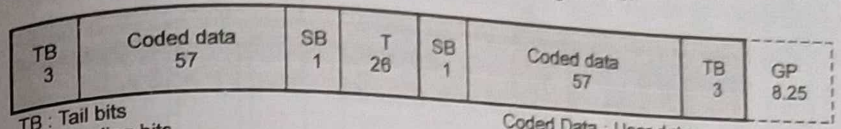
Dedicated Control Channels (DCCHs)

- The Dedicated Control Channels (DCCHs) come into play after call is established. These channels are bidirectional and have same formats and functions in both forward and reverse links.
- The DCCHs include three different types of channels :

1. Fast Associated Control Channel (FACCH)
2. Slow Associated Control Channel (SACCH)
3. Stand-alone Control Channel (SDCCH)

1. Fast Associated Control Channel (FACCH) :

- The bidirectional FCCH is used for exchange of time critical information between mobile and base station during the progress of a call. A FACCH will spread over eight slots spread out over eight frames.
- The information in FACCH and SACCH is same. The FACCH is assigned whenever SACCH has not been dedicated to a Mobile Station (MS) and there is urgent message such as handoff is requested. The FACCH transmits control information by stealing capacity from the associated traffic channel. This is done by setting two special bits called stealing bits, in TCH forward channel burst. If stealing bit is set, the time slot is known to contain FACCH data for that frame. The normal burst with stealing bits is shown in Fig. 3.2.16.



TB	Coded data	SB	T	SB	Coded data	TB	GP
3	57	1	26	1	57	3	8.25

TB : Tail bits
SB : Stealing bits
T :Training sequence
Coded Data : User data
GP : Guard Period.

Fig. 3.2.16 Normal burst

2. Slow Associated Control Channel (SACCH)

- Slow Associated Control Channel (SACCH) is used to inform base of power measurements mode by the mobile of signal strength in adjacent cells. The SACCH is transmitted on every 26 bursts of every speech when half rate is used.
- The SACCH is a bidirectional channel. It exchanges control information between base station and mobile station during a call or call setup. Various information and control signals in uplink and downlink are :

Downlink (forward channel) :

i) Broadcast messages.

ii) Power control information.

iii) Timing advance in downlink.

Uplink (reverse channel) :

i) Measurement report.

ii) Acknowledged power control.

iii) Acknowledgement of timing advance.

iv) Received signal strength and quality of TCH.

3. Stand-alone Dedicated Control Channels (SDCCH) :

- The Stand-alone Dedicated Control Channel (SDCCH) is assigned for each mobile station. The SDCCH is a bidirectional logical channel, consisting of four time slots (carrying one massage) in every multiframe. This makes transmission speed slower, but it is sufficient for the information that needs to be sent.
- The SDCCH carries signalling data following the connection of the mobile with the Base Station (BS) and just before allocation of TCH by the Base Station (BS) to the MS. The SDCCH, ensures that the MS and BS remains connected whereas BS and MSC verify subscriber unit and allocate resources for the mobile. It is a channel which accepts a newly completed call from the BCH and holds the traffic while waiting for the BS to allocate to TCH channel.

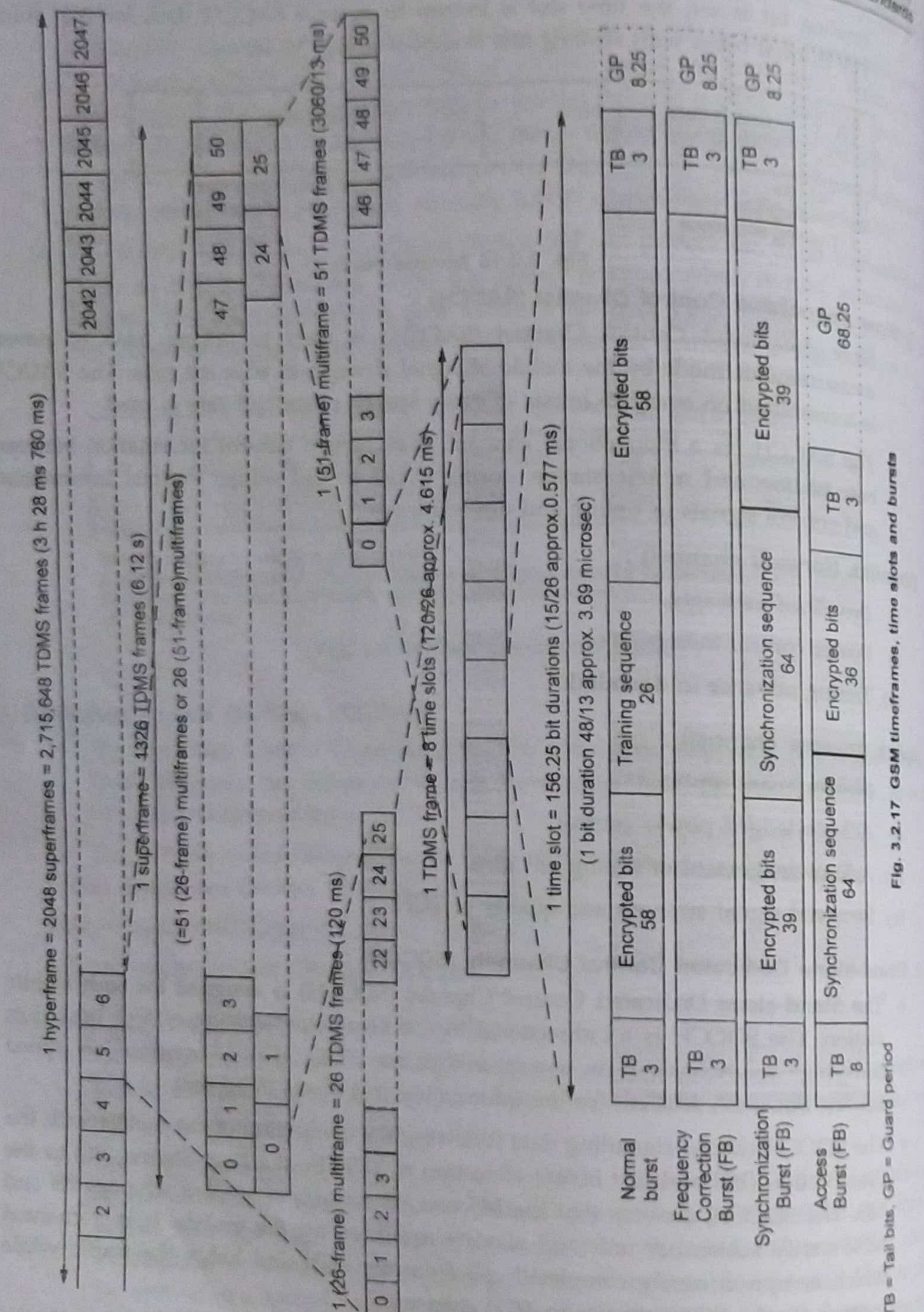

1 hyperframe = 2048 superframes = 2,715,648 TDMS frames (3 h 28 ms 760 ms)
2
3
4
5
6
2042
2043
2044
2045
2046
2047
1 superframe = 1326 TDMS frames (6.12 s)
(=51 (26-frame) multiframes or 26 (51-frame)multiframes)
0
1
2
3
47
48
49
50
0
1
24
25
1 (26-frame) multiframe = 26 TDMS frames (120 ms)
0
1
2
3
22
23
24
25
1 (51-frame) multiframe = 51 TDMS frames (3060/13 ms)
0
1
2
3
46
47
48
49
50
1 TDMS frame = 8 time slots (120/26 approx. 4.615 ms)
1 time slot = 156.25 bit durations (15/26 approx.0.577 ms)
(1 bit duration 48/13 approx. 3.69 microsec)
Normal burst
TB 3
Encrypted bits 58
Training sequence 26
Encrypted bits 58
TB 3
GP 8.25
Frequency Correction Burst (FB)
TB 3
TB 3
GP 8.25
Synchronization Burst (FB)
TB 3
Encrypted bits 39
Synchronization sequence 64
Encrypted bits 39
TB 3
GP 8.25
Access Burst (FB)
TB 8
Synchronization sequence 64
Encrypted bits 36
TB 3
GP 68.25
TB = Tail bits, GP = Guard period

Fig. 3.2.17 GSM timeframes, time slots and bursts

- The SDCCH is used to send authentication and alert messages as the mobile synchronizes itself with the frame structure and waits for TCH. SDCCH may be assigned their own physical channel or may occupy TS0 slot of the BCH if there is low demand for BCH or CCCH traffic.
- GSM Logical Channels are summarized in Table 3.2.1.

Traffic Channels (TCH)		Control Channels (CCH)			
Speech	Data	Broadcast CCH (BCCH)	Common CCH (CCCH)	Stand-alone Dedicated CCH (SDCCH)	Associated CCH (ACCH)
Full-rate TCH/F	TCH/F9.6	Frequency correction	Paging channel		Fast
	TCH/F4.8 TCH/F2.4	(FCCH) Synchronization (SCH)	(PCH) Random Access (RACH)		(FACCH) Slow (SACCH)
Half-rate TCH/H	TCH/H4.8 TCH/H2.4		Access Grant (AGCH)		

Table 3.2.1 GSM logical channels

- Different bursts within time slots are used for data transmission illustrated at a glance in Fig. 3.2.17. (See Fig. 3.2.17 on previous page)

3.2.7 GSM Frame Structure

- There are eight timeslots per TDMA frame. The frame period is 4.615 ms. A frame contains 1250 bits (8 × 156.25), some of them are not used.

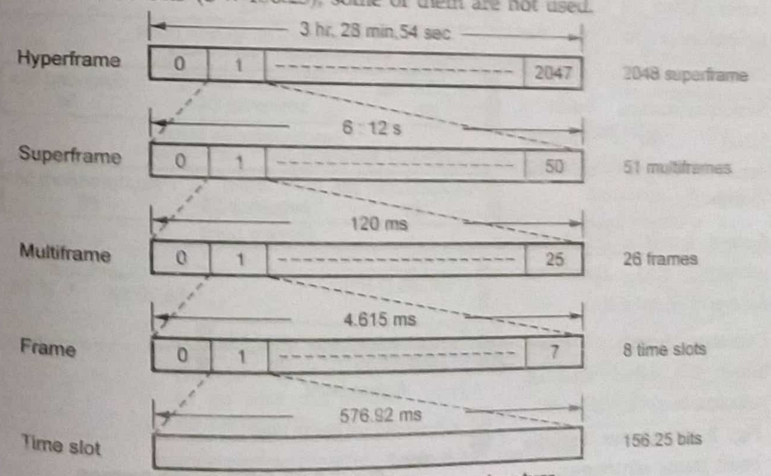


Fig. 3.2.18 GSM frame structure

- The 13th or 26th frame are not used for traffic but for control purposes. The frame rate is 216.66 frames per second or 270.833 kbps / 1250-bits / frame.
- Normal speech frames are grouped into larger structure called multiframes which forms multiframes, multiframes are grouped together to form superframes and superframes forms hyperframes. Fig. 3.2.18 shows GSM frame structure.
- A multiframe contains 26 TDMA frames one superframe contains 51 multiframes (or 1326 TDMA frames). A hyperframe contains 2048 superframes or 2,715,648 TDMA frame. A hyperframe is sent for every 3 hours, 28 minutes and 54 seconds.

3.2.8 GSM Burst Structures

- Each logical channel is realized by transmission of a specific type of data packet (burst) in the assigned time slots. Such as frequency correction, synchronization and broadcast logical channels are sent in the zero time slot of the broadcast carrier together with some other specific control channels.
- In order to realize all these channels, a normal burst, frequency correction burst and synchronization burst are emitted.
- There are 5 types of bursts :

1. **Normal burst :** used to carry information on traffic and control channels.
2. **Frequency Correction burst :** Used for frequency synchronization of the mobile.
3. **Synchronization burst :** Used for Frame synchronization of the mobile.
4. **Access burst :** Used for random and handover access.
5. **Dummy burst :** Used when no other channel requires burst to be sent.

- Fig. 3.2.19 shows various burst frame structures.

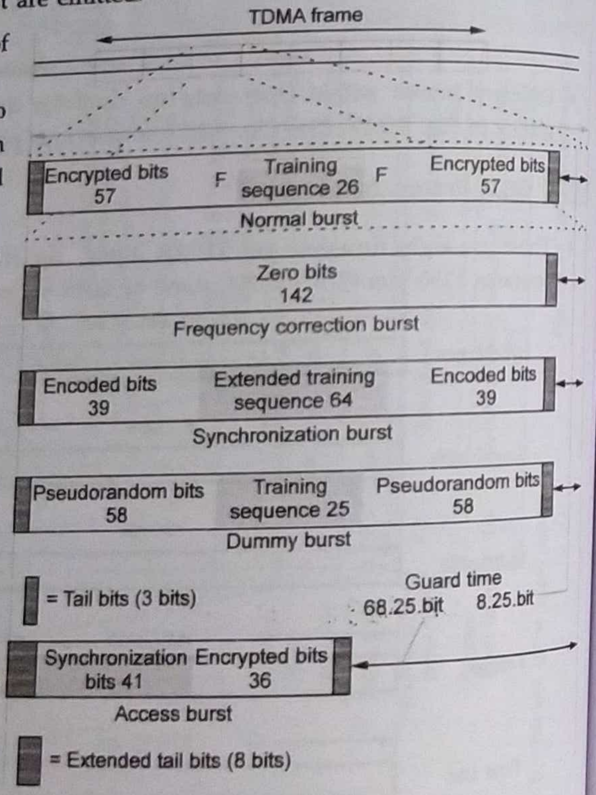


Fig. 3.2.19 GSM burst frames

- Table. 3.2.2 summarizes the burst type, its purpose, used by channels and its content.

Burst type	Purpose	Used by	Contents
Normal	Used to carry information on traffic and control channels.	BCCH, FCH, AGCH, SDCCH, CBCH, SACCH, FACCH, TCH	• Two blocks of 57 bits each for traffic. • Training sequence (26 bits) • Steal flags (1 bit each) to indicate tha! FACCH has temporarily stolen 57 bits. • Tail bits (always 000) • Guard period : 8.25 bit durations.
Frequency correction	Used for frequency synchronization of the mobile.	FCCH	• 142 frequency correction bits. • Tail bits. • Guard period : 8.25 bit durations.
Synchronization	Used for frame synchronization of the mobile.	SCH	• Two blocks of 39 bits for TDMA frame structure information. • 64 synchronization bits. • Tail bits. • Guard period : 8.25 bit durations.
Access	Used for random and handover access.	RACH FACCH	• 41 synchronization bits. • 36 bits of access information. • Tail bits. • Guard period : 68.25 bit durations. A longer GP is used because it is the first transmission from the mobile - no timing advance information is available.
Dummy	USed when no other channel requires a burst to be sent and carries no information.	All free TS on C0. (1-7)	• Pattern consists of training sequence and a mixed bits pattern.

Table 3.2.2

3.2.9 Authentication and Security in GSM

- GSM is a public system operating on radio frequencies. The information on the air interface needs to be protected to provide user data confidentiality (including speech) and to present fraudulent access and ensure subscriber privacy.
- The basic security mechanisms include :

1. User authentication ; to prevent access by unregistered users.
2. Radio path encryption ; to prevent unauthorized listening.
3. User identity protection ; to prevent subscriber location disclosure.

- In GSM, the mobile station consists of two parts : One the hardware and software specific to radio interface and second part contains the user specific data known as Subscriber Identity Module (SIM).
- SIM has several functions and limited programs are possible by user. Most of the information contained in the SIM is protected against alteration. Because of security functions duplication of SIM is difficult as these provides a high degree of protection against fraudulent access to the network.
- The basic security aspects supported by the GSM SIM are :

1. Authentication algorithm (A_3) 2. Subscriber authentication key (K_i)
3. Cipher key generation algorithm (A_8) 4. Cipher key (K_c)
5. Control of access to SIM stored data and functions performed in the SIM.

- SIM storage capability includes following data :

1. Administrative information : This indicates the SIM mode of operation (normal, type approval)
2. IC card identification : This is the number that uniquely identifies the SIM and the card issues.
3. SIM service table : This indicates optional services that are provided by SIM.
4. Information mobile subscriber identity : This unambiguously identifies subscriber.
5. Location information : This comprises the Temporary Mobile Subscriber Identity (TMSI) and Location Area Information (LAI).
6. Cipher key and cipher key sequence number : The cipher key is a sequence of symbols needed to encrypt or decrypt carried information.
7. Broadcast control channel information : This is the list of carrier frequencies to be used for call selection.

8. Forbidden PLMNs : These are held by the SIM to avoid unnecessary registration attempts.
9. Language preference : This indicates the Man-Machine Interface (MMI) languages preferred by subscriber.

3.2.9.1 Authentication

- In order to prevent fraudulent use of subscriber and mobile identities, GSM uses two methods.

1. Use of personal identity number (typically 4-digit) which is stored in SIM. A user wishing to make a call enters the PIN which is checked by SIM, without transmission on the radio interface.
2. In this stage, GSM interrogates the units. This is controlled from MSC/VLR and occurs at call set-up, location updating, handover etc.

- After the mobile user has made on access and service request, the network checks the identity of the user by sending a Random Number (RAND) of 128-bits to the mobile. The mobile uses the RAND, K_i and A_3 algorithm to produce 32-bit signed response (SRES). The network uses the same RAND, K_i and A_3 algorithm to produce a SRES which is then checked against the response from the mobile and access continues only if the two response match. The GSM authentication procedure is illustrated in Fig. 3.2.20.

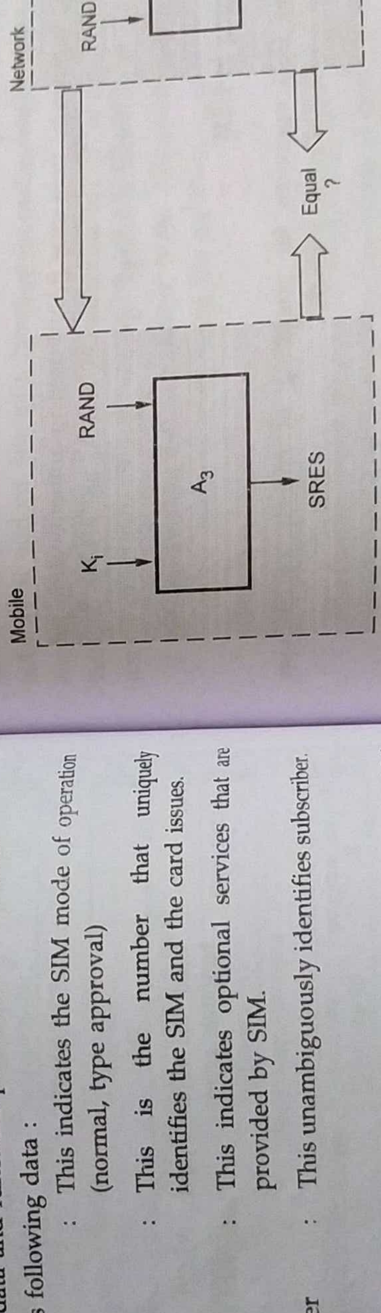


Fig. 3.2.20 GSM authentication procedure

- In order to maintain desired security level, A_3 is devised so that computation of SRES from RAND and K_i is straight forward but the computation of K_i from RAND and SRES is complex. A_3 is operator dependent, which is a further reason for performing the network SRES computation at mobile HLR.

- Authentication of mobile users can be carried out on both mobile originated call and mobile terminated call set-up, on location updating, and on activation of supplementary services. As the authentication sets are used up in VLR, further sets are requested from the HLR.

3.2.9.2 Ciphering / Encryption

- Ciphering or encryption is employed in GSM to prevent unauthorized listening. Encryption is used for all data transmitted between mobile and base station in dedicated state. It includes user information (voice, data), user related signalling (handover signalling) (called numbers) and system related signalling (handover signalling).
- Ciphering is achieved by "exclusive OR-ing" the 114 data bits of each normal burst with a pseudo random sequence. Deciphering follows exactly the same operation and reproduces the original 114-bit data ("exclusive OR-ing twice with the same pseudo random reproduces the original data stream".) The algorithm employed for generating pseudo random sequence is known as A_5 and cipher key generation is algorithm is known as A_8.
- The A_5 algorithm generates the pseudo random sequence from two inputs one being the frame number (22-bits) and other being a key K_c (64-bits) between mobile and network. Two different pseudo random sequences are generated by A_5 both for uplink and downlink.
- K_c is actually computed during GSM authentication process. It is stored in non volatile memory of SIM. It is therefore remembered after the mobile is switched off. The value of K_c is generated from same RAND used in authentication process by a secret algorithm known as A_8. The algorithms A_3 and A_8 are always together and in most cases are implemented as a single operator specific algorithm known as A_3 / A_8.

3.2.10 Signal Processing in GSM

- Fig. 3.2.21 illustrates GSM operations for processing of speech signal from transmitter to receiver over logical traffic channels.

1. Speech coding

- GSM speech coder uses Residually Excited Linear Predictive coder (RELP) along with LongTerm Predictor (LTP). The RELP provides 260-bits for each 20 ms blocks of speech which gives bit rate of 13 kbps.
- Normally a person speaks on average for less than 40 % of the time. Therefore, GSM system can operate in Discontinuous Transmission Mode (DTX) by incorporating Voice Acitivity Detection (VAD) in speech coder. This provides longer battery life for subscriber and reduces radio interference.

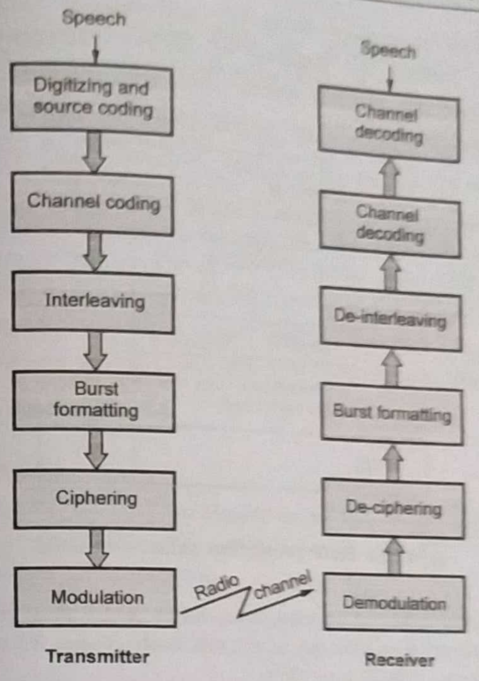


Fig. 3.2.21 GSM speech signal processing

- At receiving end a Comfort Noise Subsystem (CNS) introduces background acoustic noise to compensate for the annoying switched muting occuring due to DTX.

2. Channel coding

- The speech coder output bits are grouped for error protection, according to their significance in speech quality. The quality of speech produced by encoding the bits in 260-bit block can be divided into three classes -

1. Class Ia : 50-bits (Most sensitive to bit errors)
2. Class Ib : 132-bits (Moderately sensitive to bit errors)
3. Class II : 78-bits (Least sensitive to bit errors)

- In class Ia type 3 parity check (CRC) bits are added to them to facilitate detection of noncorrectable errors at receiver. The next 132-bits with these 50-bits + 3 CRC bits are reordered and appended by four trailing zero bits making a total 189-bits block. This block is encoded using 1/2 convolutional encoder with constraint length K = 5, making this sequence of 378-bits. The error protection coding increases the data rate of GSM speech signal with channel coding to 22.8 kbps. The error protection scheme for speech signals in GSM is shown in Fig. 3.2.22.

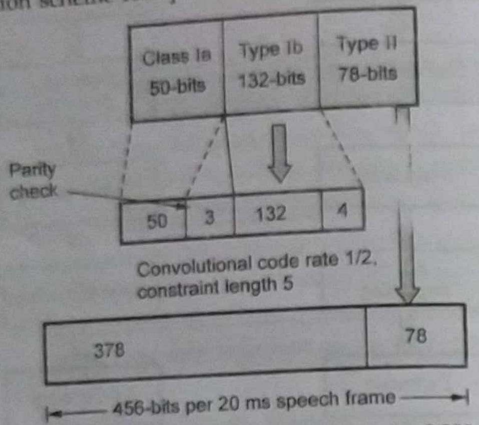


Fig. 3.2.22 Error protection scheme in GSM

3. **Interleaving**

- For minimizing the effect of sudden fades on received data, the total 456 encoded bits are broken into 8 sub-blocks of 57 bits each. These 8 sub-blocks are spread over eight consecutive TCH time slots.
- If any burst is lost due to interference or fading, channel coding ensures that enough bits will still be received correctly to allow error correction to work. A TCH time slot carriers two 57-bits of data from two different 20 ms speech segment. Fig. 3.2.23 shows diagonal interleaving of TCH/SACCH/FACCH data (speech frames) within time slots.

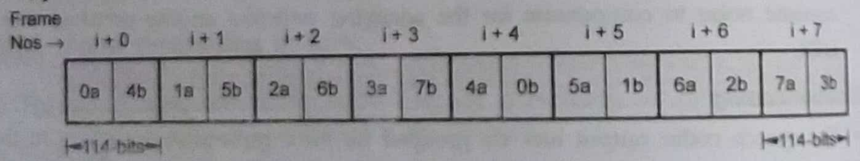


Fig. 3.2.23 Diagonal interleaving

4. **Ciphering**

Ciphering modifies the contents of eight interleaved blocks by using encryption techniques. In order to enhance security, different encryption algorithms are used for different calls. Ciphering algorithms A3 and A5 are used to prevent unauthorized network access and radio privacy respectively. A3 algorithm provides authentication to each mobile by verifying passcode within SIM with cryptographic key at MSC. A5 algorithm provides scrambling for 114 coded data bits sent in each TS.

5. **Burst formatting**

- Burst formatting adds binary digits to ciphered blocks in order to help synchronization and equalization of received signal.

6. **Modulation**

- GSM uses 0.3 GMSK modulation where 0.3 describes the 3 dB bandwidth of Gaussian pulse shaping filter with relation to the bit rate (BT = 0.3).
- GMSK is a special digital FM modualtion. Binary ones and zeros are represented in GSM by shifting RF carrier by ± 67.708 kHz. The GSM channel data rate is 270.833333 kbps, which is four times RF carrier shift. This minimizes the BW occupied by modulation spectrum which improves channel capacity.
- The MSK modulated signal is passed through Gaussian filter to eliminate rapid frequency transitions so that it will not spread energy into adjacent channels.

3.2.11 GSM Call Procedure

3.2.11.1 Call from Mobile

- A channel is requested on RACH and may be in contention with other mobile by using slotted ALOHA. If a request is received without a collision a dedicated control channel AGCH is assigned.
- On receiving access grant, mobile proceeds with call setup on the allocated dedicated control channel by sending setup message to network. The network accepts the call establishment on SDCCH .
- When called party alerting has been initiated, an alerting message is sent to the mobile over the FACCH and a ringing tone may be generated by the network and sent to mobile.
- When call has been accepted at the remote end, a connect message is transferred to the mobile, indicating that the connection is established in the network. The mobile station responds by sending connect acknowledge message and enters in active state.

Sr.No	System activity	Channel	Mobile activity
1.	System overhead parameters and other overhead messages.	BCCH ⇨	(Idle Updated) monitor BCCH and CCCH (PCH) for mobile control message.
2.	Receive channel request.	⇦ RACH	Generate channel request.
3.	Assign stand alone dedicated control channel.	AGCH ⇨	Receive stand alone dedicated control channel assignment and store in memory.

4.	Receive call establishment request.	← SDCCH	Send call establishment request.
5.	Request authentication from mobile.	SDCCH →	Receive authentication request.
6.	Receive and check authentication.	← SDCCH	Authentication response.
7.	Request mobile to transmit in ciphered mode.	SDCCH →	Receive cipher mode request.
8.	Receive acknowledgement.	← SDCCH	Acknowledge cipher mode request (all further transmission in cipher mode).
9.	Receive setup request.	← SDCCH	Send setup message and desired number.
10.	Send call proceeding indication to mobile and route call to desired number.	SDCCH →	Receive call preceeding indication.
11.	Assign traffic channel to mobile.	SDCCH →	Receive traffic channel assignment.
12.	Receive traffic channel acknowledgement on allocated channel.	← FACCH	Switch to traffic channel and send an acknowledgement.
13.	Send alert signal that called number is available and the phone is ringing.	FACCH →	Receive alert signal ringing sound.
14.	Send connect message when called party accepts.	FACCH →	Receive connect message.
15.	Receive connect accept response.	← FACCH	Acknowledge connect message and switch to traffic channel.
16.	Exchange of user data.	↔ TCH	Conversation commences on TCH.

Table 3.2.3 Call establishment from a mobile

3.2.11.2 Call to Mobile

- A paging message is routed to the traffic area in while the mobile is registered and transmitted on paging channel.
- When access grant is received from the base station the mobile responds with call confirmed message on dedicated control channel. A traffic channel is then allocated and call proceeds.

Sr.No	System activity	Channel	Mobile activity
1.	System overhead parameters and other overhead messages.	SDCCH →	(Idle Updated) monitor BCCH and CCCH (PCH) for mobile control message.
2.	Receive incoming call, generate a paging message.	BCCH →	Receive paging message.
3.	Receive channel request .	PCH →	Generate channel request.
4.	Assign stand alone dedicated control channel.	← RACH	Receive stand alone dedicated control channel assignment and store in memory.
5.	Receive paging acknowledgement.	AGCH →	Answer paging message from network.
6.	Request authentication from mobile.	← SDCCH	Receive authentication request.
7.	Receive and check authentication.	← SDCCH	Authentication response.
8.	Request mobile to transmit in ciphered mode.	SDCCH →	Receive cipher mode request.
9.	Receive acknowledgement.	← SDCCH	Acknowledge cipher mode request, switch to cipher mode.
10.	Send setup message of incoming call.	SDCCH →	Receive setup message.
11.	Assign traffic channel to mobile.	SDCCH →	Receive traffic channel assignment.
12.	Receive traffic channel acknowledgement on allocated channel.	← FACCH	Switch to traffic channel and send an acknowledgement.
13.	Send alert signal.	FACCH →	Receive alert signal and generate ringing sound.
14.	Send connect message when user off-hook.	FACCH →	Receive connect message.

15.	Receive connect accept response.	FACCH	Acknowledge connect message and switch to traffic channel.
16.	Exchange of user data.	TCH	Conversation commences on TCH.

Table 3.2.4 Call establishment to a mobile

3.2.11.3 Call Setup

- Call setup in GSM consists of certain necessary operations. Some of the operations are -

1. Interrogation phase
2. Radio resource connection establishment
3. Service request
4. Authentication
5. Ciphering mode setting
6. IMEI check
7. TMSI reallocation
8. Call initiation procedure
9. Assignment of a traffic channel
10. Call confirmation, call accepted and call release

3.2.11.4 Radio Resource Connection Establishment

- The MSC/VLR initiates the call setup process by sending a message to the appropriate BSC. The BSC sends a paging command message to the appropriate BTS, finally BTS sends a paging request to the appropriate MS.
- Steps involved in radio resource connection establishment phase are-

1. The MSC initiates the call setup process by sending paging message to BSC.
2. The BSC sends paging command message to appropriate BTSs.
3. The BTS sends a paging request message to MS on PCH.
4. The MS responds to paging request message by sending a channel request message to BTS on RACH.
5. BTS sends a channel required message to BSC.
6. BSC sends channel activation message to BTS.
7. BTS acknowledges the channel activation message.

8. BSC sends an immediate assignment command message to BTS.
9. The immediate assign command is sent by BTS to MS over AGCH.

- Fig. 3.2.24 illustrates steps involved in radio resource connection establishment.

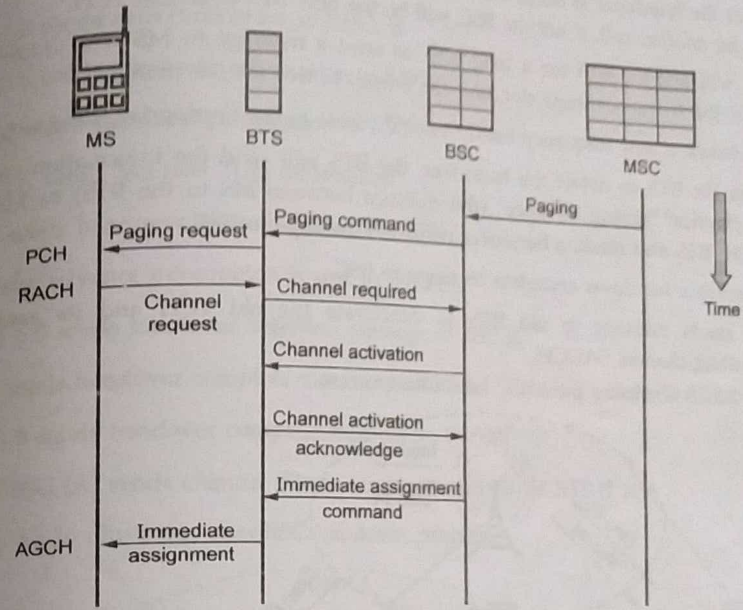


Fig. 3.2.24 Messaging during GSM radio resource connection establishment

3.2.12 GSM Handoff Procedure

- Handoff or handover occurs when an active MS changes cells. BSC of the location initiates handover. Several different types of handover scenarios are possible, such as

1. Intra-BSC handover
2. Inter-BSC handover
3. Inter-MSC handover

3.2.12.1 Intra-BSC Handoff / Handover

- The intra-BSC handover process involves following steps.

1. The intra-BSC handoff occurs between two cells controlled by BSC. During the call, MS will measure the strength and quality of the signal on the TCH and signal strength from the neighboring cells. MS will evaluate and assess the Received Signal Strength (RSS) average for each cell.

2. The BTS will send the results of measurements on the TCH to the BSC. In the BSC, the function is activated when the placement is required to handover to another cell.
3. When the handover is done, BSC will check whether the channel had requested be met by another cell, if not the BSC will be the new BTS to enable TCH.
4. BSC will ask the BTS for a long time to send a message to MS with information about the frequency, time slot, and the output power for the change.
5. MS choose a new frequency handover and access to the appropriate time slot.
6. When the BTS to detect the handover, the BTS will send the information contains the physical "timing advance" (the distance between MS to the BTS) to MS over FCCH. BTS also sends a handover detection message to BSC.
7. MS sends a handover complete message to BSC.
8. BSC sends message to old BTS to deactivate the old TCH and its associated signalling channel SACCH.

- Fig. 3.2.25 illustrates intra-BSC handover process.

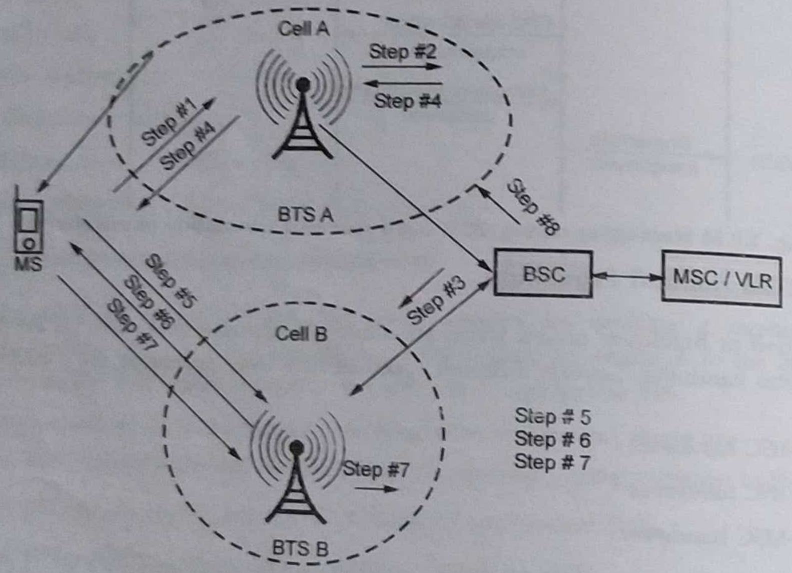


Fig. 3.2.25 Intra-BSC handover

3.2.22 Inter-BSC Handoff

- In inter-BSC handover, the mobile has moved to a cell that is in different location area and therefore has different BSC. The serving BSC decides that the call must be handed over to a new cell that belongs to different BSC.

- The inter-BSC handover process involves following steps.

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

- Fig. 3.2.26 illustrates inter-BSC handover process.

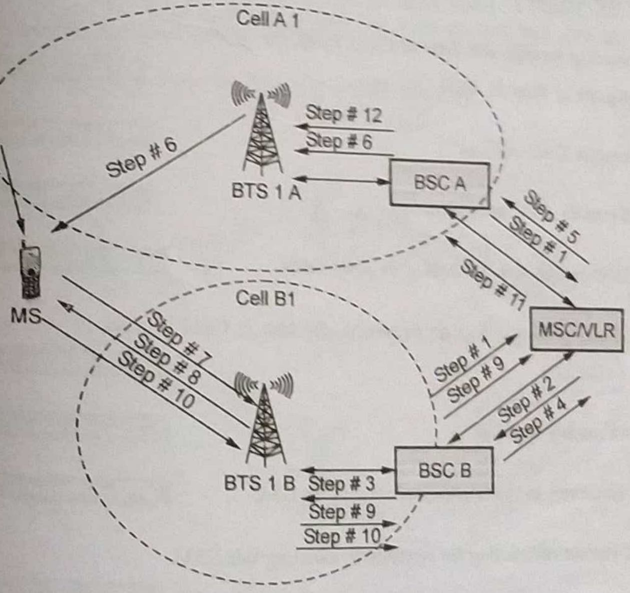


Fig. 3.2.26 Inter-BSC handoff

- The basic difference between intra-BSC handover and inter-BSC handover is that two BSCs and the MSC are involved in an inter-BSC handover while the intra-BSC handover involves only two BTS connected to the same BSC.

University Questions

1. *Explain functional architecture of GSM system. And also give different tele-services provided by GSM.* GTU : Winter-11, Marks 7
2. *What are the possible handover scenarios in GSM ? List out the numbers needed to locate a mobile station and to address the mobile station.* GTU : Winter-11, Marks 7
3. *What are HLR and VLR ? Describe its functions in call routing and roaming.* GTU : Summer-12, Marks 6
4. *What are the services provided by supplementary services ?* GTU : Winter-12, Marks 3
5. *What is the frequency range of uplink and downlink in GSM network ?* GTU : Winter-12, Marks 2
6. *What are the four possible handover scenarios in GSM ?* GTU : Winter-12, Marks 2
7. *How is mobility management done in GSM ? List the various handovers carried out in GSM and explain any one of them in detail.* GTU : Winter-12, Marks 7
8. *List and explain GSM entities.* GTU : Winter-13, Marks 7
9. *Draw and explain GSM architecture.* GTU : Winter-13, Marks 7
10. *Explain GSM architecture and role of its components.* GTU : Summer-14, Marks 7
11. *What is cellular network ? Explain frequency allocation in GSM network.* GTU : Summer-14, Marks 4
12. *Explain call routing in GSM.* GTU : Summer-14, Marks 4
13. *Explain : Handover, authentication and security in GSM.* GTU : Summer-14, Marks 4
14. *Draw and explain call routing for a mobile terminating call GSM.* GTU : Winter-14, Marks 7

3.3 General Packet Radio Service (GPRS)

GTU : Winter-11, 13, Summer-12,13, 14,15

- General Packet Radio Service is an overlay on top of GSM physical layer and network entities. GPRS system is used by the GSM mobile phones.
- The GPRS network acts in parallel with the GSM network, providing packet switched connections to the external networks.
- A GPRS network must provide all of the functionality of a GSM network for packet switched networks and more.
- Frequency spectrum of GSM is used overlayed on the traffic channel of GSM.
- GPRS short packets of 500 - 1000 bytes have short access time.

GPRS Speed

- GPRS can theoretically use one to eight of the GSM timeslots for uplink and downlink traffic.
- The capacity ranges from 9.05 kbps to 21.4 kbps where the slower ones provide varying amounts of error correction.

GPRS Devices

- GPRS device are expected to be in many different kinds, shapes and functionality. However, all GPRS devices can be divided into three different categories :

1. **Class A** devices can operate GPRS simultaneously with other GSM services (such as a normal voice call).
2. **Class B** devices can operate both GPRS and GSM services but not at the same time. The device must shift between the two modes but can be registered in the network for both.
3. **Class C** devices operate exclusively GPRS services.

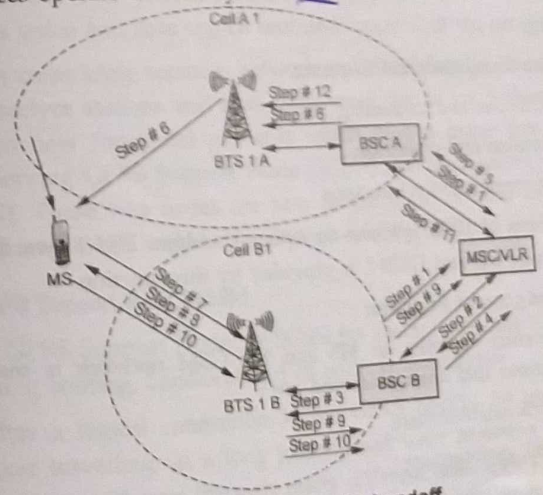


Fig. 3.3.1 Inter-BSC handoff

3.3.1 GPRS Functional Groups

- The functions defined in GPRS are as following.

1) Network access function

2) Packet routing and transfer

3) Mobility management

4) Logical link management

5) Radio resource management

6) Network management

1. Network Access Function :

- Main functions of network access function include :
  - Point to point data transfer,
  - Authentication and authorization
  - Admission control
  - Message screening
  - Registration of MS with packet data protocols,
  - Radio resources for MS communication and
  - Charging information about packet transmission

2. Packet Routing and Transfer Function :

- Packet routing and transfer function route the data between an MS and the destination through the serving and gateway GPRS Support Nodes (GSNs).
  - Relay function
  - Routing
  - Address translation and mapping
  - Encapsulation and tunnelling
  - Compression and ciphering
  - Domain name service functions
  - Conversion of GPRS address to external address and forwarding of packets between an MS and GGSN, is provided by this function.

3. Logical Link Management Function :

- The communication between an MS and the GSM network is maintained by it. The main functions that are maintained are :
  - Logical link establishment
  - Logical link maintenance
  - Logical link release

4. Radio Resources Management Function :

- Radio communication paths are allocated by it. The main functions that are maintained are :
  - Um management
  - Cell selection
  - Um-tranx, which provides packet data transfer capability such as Medium access control, etc.
  - Path management

5. Mobility Management Function :

- Current location of an MS is kept by it. When an MS is entered to a new area, all routing and location in formations are also updated by it. The main functions that are maintained are -
  - Keeps track of the current location of an MS
  - Cell update, routing area update, combined
  - Routing area and location area update

6. Network Management Function :

- If provides mechanisms to support network functions related to GPRS. An important function performed is that it provides mechanism to support OA&M functions.

3.3.2 GPRS Architecture

- The GSM network still provides voice and the GPRS network handles data, because of this voice and data can be sent and received at the same time.
- GPRS is not a completely separate network to GSM. Many of the devices such as the base transceiver stations and base transceiver station controllers are still used. There are two new functional elements which play a major role in how GPRS works. The Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). These two nodes are new to the network with the other changes being small if any. GPRS architecture is shown in Fig. 3.3.2.

3.3.2.1 Serving GPRS Support Node (SGSN)

- The Serving GPRS Support Node, or SGSN for short, takes care of some important tasks, including routing, handover and IP address assignment.
- The SGSN has a logical connection to the GPRS device. As an example, if you where in a car travelling on a long journey and were browsing the Internet on a GPRS device, you will pass through many different cells. One job of the SGSN is to make sure the connection is not interrupted as you make your journey passing

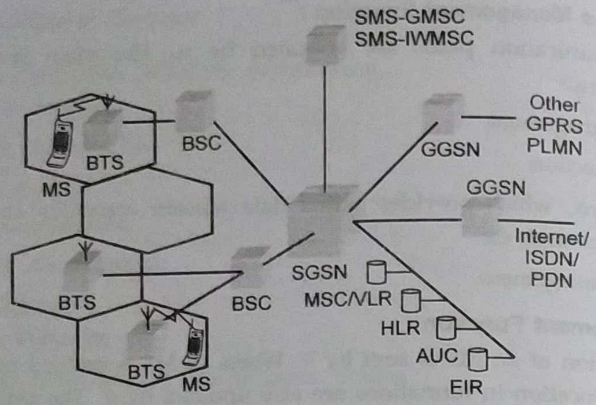


Fig. 3.3.2 GPRS architecture

from cell to cell. The SGSN works out which BSC to "route" your connection through.

- If the user moves into a segment of the network that is managed by a different SGSN it will perform a handoff of to the new SGSN, this is done extremely quickly and generally the user will not notice this has happened. Any packets that are lost during this process are retransmitted.
- The SGSN converts mobile data into IP and is connected to the GGSN via a tunnelling protocol.

3.3.2.2 Gateway GPRS Support Node (GGSN)

- The gateway GPRS support node is the "last port of call" in the GPRS network before a connection between an ISP or corporate network's router occurs.
- The GGSN is basically a gateway, router and firewall rolled into one. It also confirms user details with RADIUS servers for security, which are usually situated in the IP network and outside of the GPRS network.

3.3.2.3 Connectivity between the SGSN and GGSN

- The connection between the two GPRS support nodes is made with a protocol called GPRS. Tunnelling Protocol (GTP). GTP sits on top of TCP/IP and is also responsible for the collection of mediation and billing information.
- GPRS is billed on per megabyte basis unlike GSM. In practice the two GSN devices may be a single unit.

3.3.2.4 HLR

- The HLR or Home Location Register is a database that contains subscriber information, when a device connects to the network their MSISDN number is associated with services, account status information, preferences and sometimes IP addresses.

3.3.2.5 Air Interface

- GPRS is a packet switching data service, overlaid on the GSM infrastructure.
- GPRS service can be grouped into 3 classes :

a) **Class A :** Simultaneous use of data and voice services. Thus class A service allows a user to hold a conversation and transfer GPRS data at the same time.

b) **Class B :** Supports simultaneous GSM and GPRS attach but not simultaneous use of both services. Thus a class B user can be registered on both services at the same time, but cannot use both services at the same time.

c) **Class C :** Can attach to only one service at a time.

- As mentioned earlier, GPRS allows access to multiple slots. It is also asymmetric in the sense that downlink slots may be greater than uplink slots since higher data rates are needed during download operation. Table 3.3.1 shows common multi-slot class.

Multi-slot class	Download slots	Uplink
2	2	1
4	3	1
8	4	1
12	4	2

Table 3.3.1

- GPRS uses the same air interface as GSM i.e. 200 kHz RF Carrier and 8 Timeslots, however, at any given time, same of the slots may be carrying voice and same data. This is achieved by using a different logical channel allocation and coding scheme.

3.3.3 GPRS Network Service

- GPRS provides the following network services :

1. **Point-to-multipoint (PTM-M) :** Multicast services for subscribers in given area.
2. **Point-to-multipoint group (PTM-G) :** Multicast service to predetermined group that may be spread over geographic area.
3. **Point-to-point (PTP) :** Packet data transfer (connectionless and connection oriented)

- GPRS performance parameters are specified on the basis of different reliability cases and delay classes.
- Three reliability cases are defined as shown in Table 3.3.2.

	Probability for			
Class	Lost packet	Duplicated packet	Out-of-sequence packet	Corrupted packet
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}

Table 3.3.2

- Delay classes are summarized in Table 3.3.3.

	128 Byte packet		1,024 Byte packet	
Class	Mean Delay	95 % Delay	Mean Delay	95 % Delay
1.	< 0.5s	< 1.5s	< 2s	< 7s
2.	< 5s	< 25s	< 15s	< 75s
3.	< 50s	< 250s	< 75s	< 375s
4.	Best effort	Best effort	Best effort	Best effort

Table 3.3.3

3.3.4 Mobility Supports in GPRS

- Similar to CDPD and GSM, GPRS also has mechanisms to support mobility.

3.3.4.1 Attachment Procedure

- Before accessing GPRS services, the MS must register with the GPRS network and become "known" to the PDN.
- The MS performs an **attachment procedure** with an SGSN that includes -
  1. Authentication
  2. Check with GR etc.
- It is allocated a Temporary Logical Link Identity (TLLI) by the SGSN.
- A PDP (Packet Data Protocol) context is created for the MS.
- A user may multiple PDP contexts at any time. The PDP address may be statically or dynamically assigned. This PDP context is used to route packet accordingly.

3.3.4.2 Location and Handoff Management

- The location and handoff management procedures in GPRS are based on tracking of MSs location and ability to route packets to it accordingly.
- The location management depends on three states of MS : IDLE, STANDBY and READY as shown in Fig. 3.3.3.

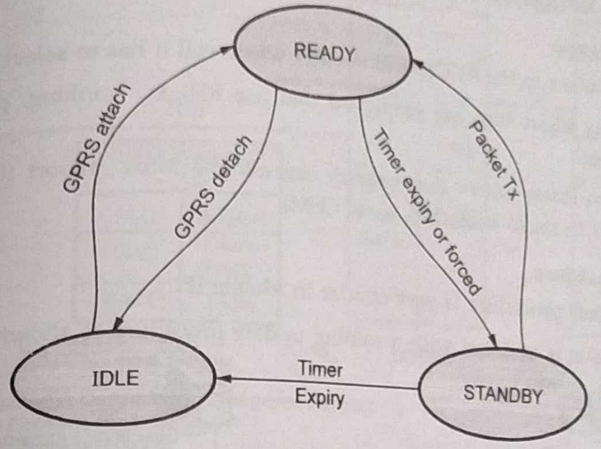


Fig. 3.3.3 Location management in GPRS

- In the IDLE state the MS is not reachable. Hence all PDP contexts are deleted.
- In the STANDBY state, movement across routing areas are updated to the SGSN but not across cells.
- In the READY state, every movement of the MS is indicated to the SGSN.

Why three states

- If the MS updates its location too often, it consumes battery power and wastes the air-interface resources.
- If it updates too infrequently, a system-wide paging is needed; this is also a waste of resources.
- A standby state focuses the area -chances of packets reaching are medium.
- A ready state pinpoints the area- chances of packets reaching are high.

Routing Area Updates

- Routing area updates are part of standby state.
- In intra-SGSN RA update, the SGSN already has the user profile. A new temporary mobile subscriber identity is issued as part of routing area update "accept". The home GGSN and GR (HLR) need not be updated.

- In inter-SGSN RA update, the new RA is serviced by a new SGSN. The new SGSN requests the old SGSN to send the PDP contexts of the MS. The new SGSN informs the home GGSN, the GR and other GGSNs about the user's new routing context.

3.3.4.3 Mobility Management in GPRS

1. Handoff Initiation

- The MS listens to the BCCH and decides which cell it has to select.
- Proprietary algorithms are employed that use RSS, c ranking, path loss, power budget, etc.
- An option exists where the network can ask the MS t report its measurements and ask it to make a handoff (as in GSM).

2. Handoff Procedure

- The handoff procedure is very similar to Mobile IP.
- The location is updated with a routing update procedure as shown in Fig. 3.3.4.

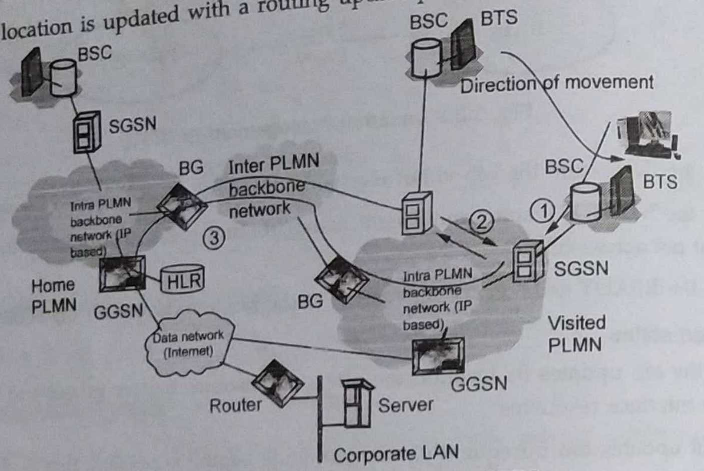


Fig. 3.3.4 Handoff management in GPRS

3. Steps in Mobility Management

i) When MS changes Routing Area (RA), it sends RA update to new SGSN.

ii) Communication between new and old SGSN.

iii) Communication between new SGSN and Home-GGSN/HLR.

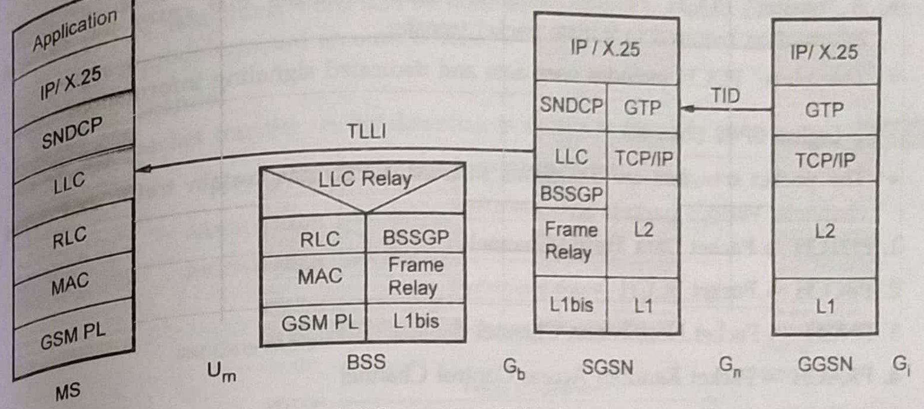
iv) The Home GGSN "tunnels" packets to the new SGSN.

v) The HLR deletes old SGSN information and includes the new SGSN information in the database.

vi) The new SGSN decapsulates packets and forwards them to the MS.

3.3.5 Transport Layers in GPRS

- GPRS protocol stack is shown in Fig. 3.3.5. This is the transport plane where data is transferred over GPRS/GSM infrastructure.



SNDCP : Subnetwork Dependent Convergence Protocol
BSSGP : BSS Gateway Protocol
GTP : GPRS Tunneling Protocol

Fig. 3.3.5 GPRS transport plane

3.3.5.1 GPRS Signaling Plane

- GPRS signaling plane enables signalling between various elements of infrastructure.
- GPRS employs out of band signaling in support of actual data transmission.
- Signaling between SGSN, HLR, VLR, EIR is similar to GSM and extends only the GPRS related functionality. Therefore it is based on Signaling System -7.
- Between the MS and SGSN, a GPRS mobility management and session management (GMM/SM) protocol is used for signaling purposes.
- Over the air, physical layer is the same as GSM (uses GMSK). Its functionalities include -

1. Forward error correction and indication of uncorrectable code words
2. Interleaving of radio "blocks"
3. Synchronization
4. Monitoring of radio link signal quality
5. Other functions similar to GSM

3.3.5.2 Medium Access

- Uplink and downlink transmissions are independent.
- Medium access protocol is called "Master-Slave Dynamic Rate Access" or MSDRA.
- Organization of time-slot assignment is done centrally by the BSS.
- A "master" PDCH includes common control channels that carry the signaling information required to initiate packet transfer.
- The "slave" PDCH includes user data and dedicated signaling information.

3.3.5.3 Logical GPRS Channels

- The packet transfers are analogous to GSM, GPRS has certain traffic and control channels. Various packets are -

1. PDTCH → Packet Data Traffic Channel
2. PBCCH → Packet BCCH
3. PNCH → Packet Notification Channel
4. PRACH → Packet Random Access Control Channel
5. PAGCH → Packet Access Grant Channel
6. PACCH → Packet Associated Control Channel (Use to send ACKs for received packets)
7. PTCCH → Packet Timing-advance Control Channel is used for adaptive frame synchronization.

Uplink Channel

- The packet transfer on the uplink is shown in Fig. 3.3.6.

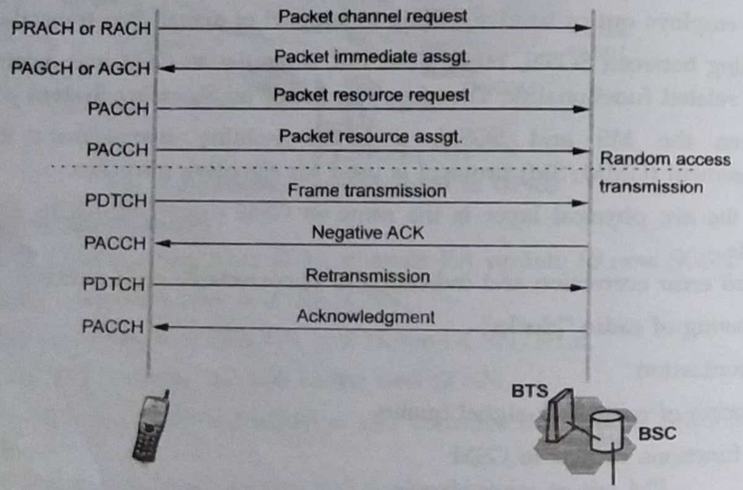


Fig. 3.3.6 Uplink data transfer

- If a MS does not get an ACK, it will back off for a random time and try again.
- The Master-Slave mechanism utilizes a 3 bit "uplink status flag" or USF on the downlink.
- A list of PDCHs and their USF are specified. The packet resource or immediate assignment message indicates what USF state is reserved for the mobile on a PDCH. Assignment can also be done so that a MS can send packets uninterrupted for a predetermined amount of time.

Downlink Channel

- The packet transfer on the downlink is shown in Fig. 3.3.7.

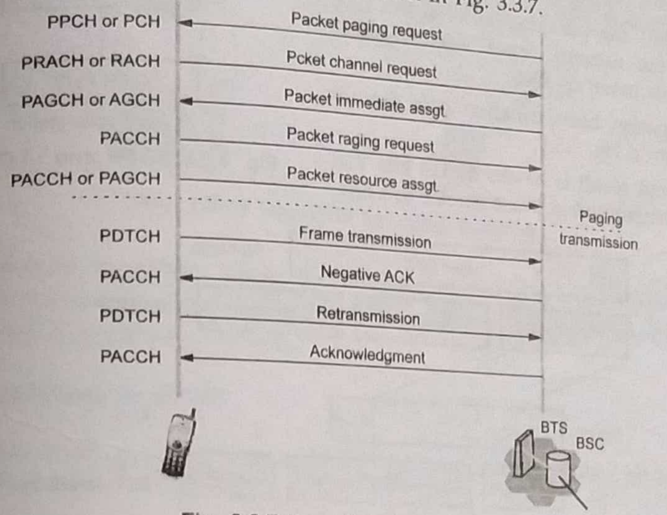


Fig. 3.3.7 Downlink data transfer

- Data transmission to a mobile can be interrupted if a high priority message needs to be sent.
- Instead of paging, a resource assignment message may be sent to the MS if it is already in a "ready" state.

Logical Link Control (LLC)

- The TLLI (Temporary Logical Link Identity) is used to identify a MS in the LLC header.
- A logical link is created between the MS and the SGSN.
- LLC performs sequence control, error recovery, flow control and encryption. It has an acknowledged mode (with retransmission for network layer payloads) and an unacknowledged mode (for signaling and SMS).
- LLC supports various QoS classes.

SNDCP

- Fig. 3.3.8 shows how packets flow from higher layers, applications and signalling levels to SNDCP and the LLC.
- It supports a variety of network protocols (IP, X.25, CLNP etc.). It multiplexes and demultiplexes the network layer payload.
- It forms the interface between the LLC and the network layer. Also, handles packets based on QoS.
- The packet transformation data flow is shown in Fig. 3.3.8.
- The end result is blocks of 114 bits that are transmitted in burst similar to GSM.

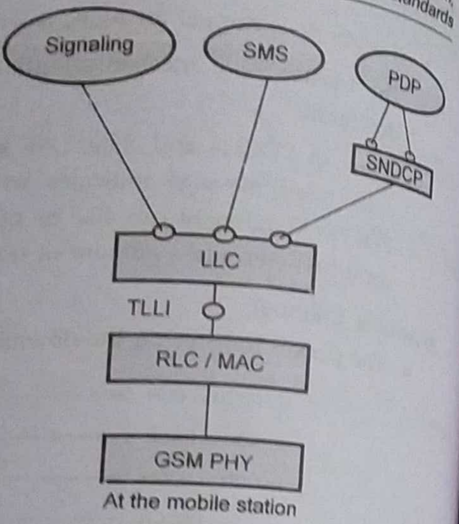


Fig. 3.3.8 SNDP and LLC in GPRS

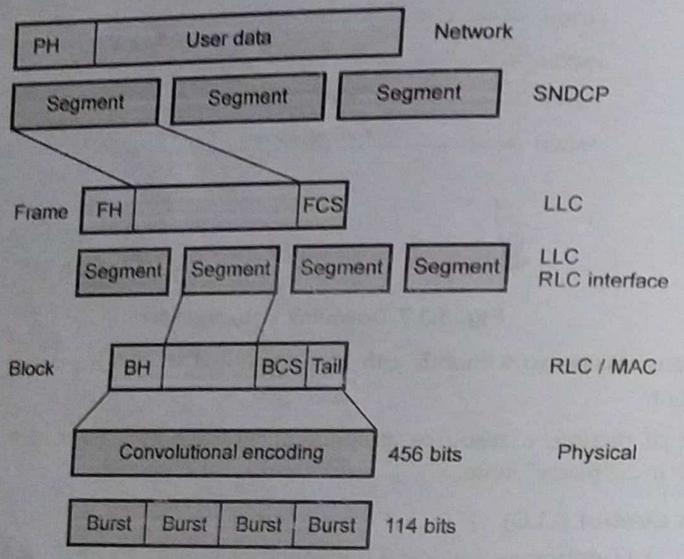


Fig. 3.3.9 Packet transformation data flow

GPRS Tunneling Protocol (GTP)

- GPRS Tunneling Protocol (GTP) allows multi-protocol packets to be tunneled through the GPRS backbone.
- A Tunnel ID (TID) is created using signaling plane that tracks the PDP context. GTP has capability of multiplexing different payloads.

- TID use in mobility management. Two level tunnelling mechanism implemented in GPRS is shown in Fig. 3.3.10.

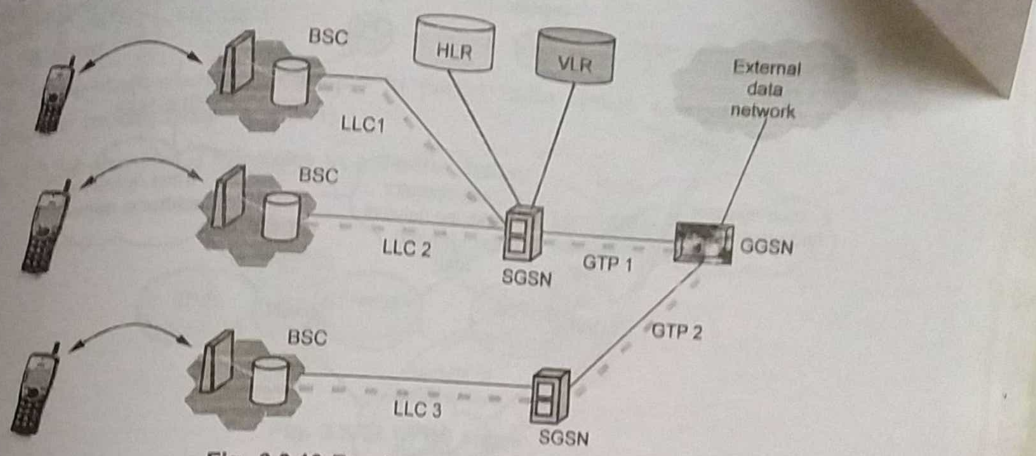


Fig. 3.3.10 Two-level tunneling in GPRS

- The two-level tunneling mechanism corresponds to a two level mobility. LLC "tunnels" (or virtual circuits) correspond to small area mobility, while GTP tunnels correspond to wide area mobility.

3.3.6 Call Routing in GPRS

- One of the main requirements in the GPRS network is the routing of data packets to and from a mobile user.
- The requirement can be divided into two areas :
  1. Data packet routing and
  2. Mobility management.

1. Data Packet Routing

- The main functions of the GGSN involve interaction with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS.
- GGSN routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS.
- GGSN 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).

Fig. 3.3.11 illustrates three routing schemes.

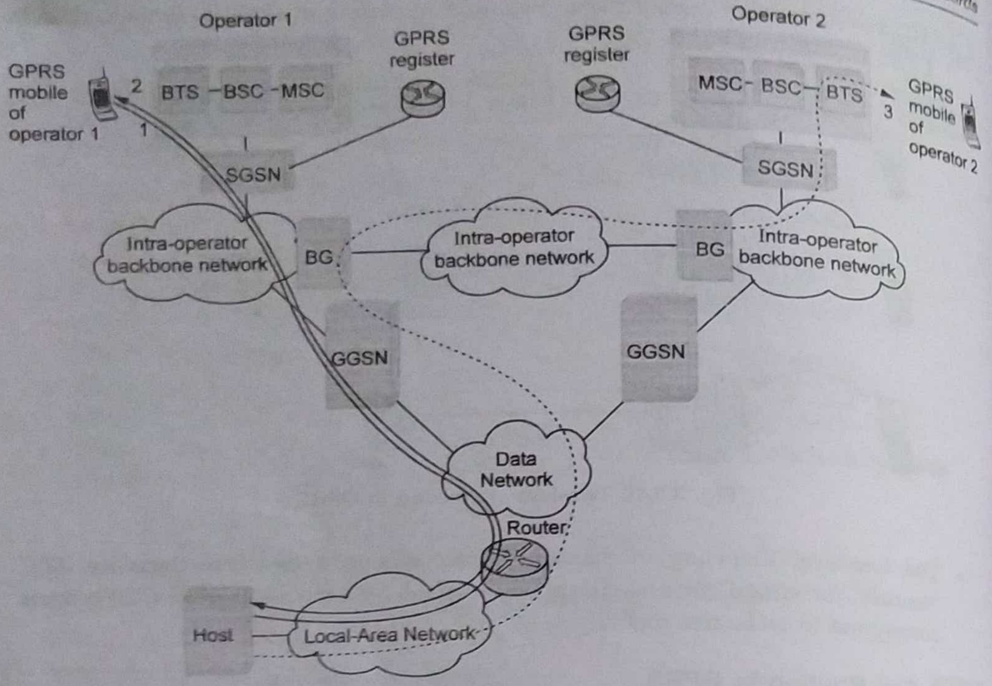

Operator 1
GPRS register
GPRS register
Operator 2
GPRS mobile of operator 1
2
1
BTS
BSC
MSC
SGSN
MSC
BSC
BTS
3
GPRS mobile of operator 2
SGSN
Intra-operator backbone network
BG
Intra-operator backbone network
BG
Intra-operator backbone network
GGSN
GGSN
Data Network
Router
Host
Local-Area Network

Fig. 3.3.11 Routing of data packets between a fixed host and a GPRS MS

1. **Mobile-originated message (path 1)**
   - This path begins at the GPRS mobile and ends at the Host.
2. **Network-initiated message when the MS is in its home network (path 2)**
   - This path begins at the Host and ends at the GPRS mobile.
3. **Network-initiated message when the MS roams to another GPRS network (path 3)**
   - This path is indicated by the dotted line.
   - The GPRS network encapsulates all data network protocols into its own encapsulation protocol called the GPRS tunneling protocol (GTP).
   - The GTP ensures security in the backbone network and simplifies the routing mechanism and the delivery of data over the GPRS network.

2. **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 has three states in the GPRS system.
  1. Active state
  2. Standby state
  3. Idle state
- The three-state model is unique to packet radio system whereas GSM uses a two-state model (idle or active).
- Fig. 3.3.12 shows GPRS states in a mobile station.

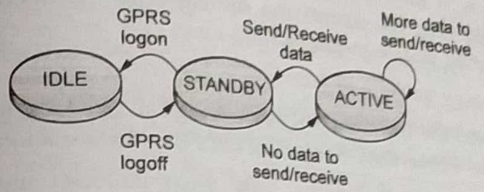


Fig. 3.3.12 GPRS states

State 1 : 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. The description of the channel (one or multiple time slots) is included in the access grant message. The data is transmitted on the reserved channels.

State 2 : 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.
- The main reason for the standby state is to reduce the load in the GPRS network caused by cell-based routing update messages and to conserve the MS battery.
- When an MS is in the standby state, the SGSN is informed of only routing area changes. By defining the size of the routing area, the operator can control the number of routing update messages.

State 3 : 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.

3.3.7 Billing and Charging in GPRS

- GPRS is essentially a packet switching overlay on a circuit switching network. The minimum charging information is collected in the Stage 1 service description. The stage 1 service description includes :
  - destination and source addresses,
  - usage of radio interface,

  - usage of external packet data networks,
  - usage of the packet data protocol addresses,
  - usage of general GPRS resources
  - location of the Mobile Station.
- GPRS network break the information to be communicated down into packets therefore it is needed to be able to count packets to charging customers for the volume of packets they send and receive.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.

- The GPRS service charging can be computed on several parameters :

1. **Volume of data :** The amount of bytes transferred downloaded and uploaded.
2. **Duration of connection :** The duration of a PDP context session.
3. **Time of session :** Date, time of day, and day of the week (enabling lower tariffs at off-peak hours).
4. **Destination :** Subscriber could be charged for access to the specific network, such as through a proxy server.
5. **Location :** The current location of the subscriber.
6. **Quality of Service :** More charges for higher network priority.
7. **SMS :** The SGSN will produce specific CDRs for SMS.
8. **Served IMSI/subscriber :** Different subscriber classes (different tariffs for frequent users, businesses, or private users).
9. **Reverse charging :** Receiving subscriber is not charged for the received data; but the sending party is charged.
10. **Free data :** Specified data to be free of charge.
11. **Flat rate :** A fixed monthly fee.
12. **Bearer service :** Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhaps the bearer service would be good for areas where it would be cheaper for the operator to offer services from a wireless LAN rather than from the GSM network.

3.3.8 Comparison of GSM and GPRS

Sr. No.	GSM	GPRS
1.	GSM has lower bandwidth compared to GPRS.	GPRS has a higher bandwidth and therefore a higher speed of data transmission.
2.	GSM service involves circuit switching channels.	GPRS networks use packet switching.
3.	In the circuit switched connection, the channel remains active even if there is no communication going on.	Much better and efficient use of bandwidth and other resources in the GPRS networks because here the bandwidth is used only when the data is being transferred.
4.	In GSM one timeslot is allocated to one MS	In GPRS multiple timeslots are allocated to one MS.
5.	In GSM signaling and traffic follow different multi frame structure. 51 frame MF is used for signaling and 26 frame MF is used for traffic.	In GPRS signaling and traffic both follow common one multi frame structure i.e. 52 frame MF structure. Here 52 Multiframe composed of total 12 radio blocks, two idle slots and two slots are for PTCCH used for timing advance purpose. Each Radio Block spans over 4 consecutive TDMA frames of one time slot.
6.	In GSM time slot is allocated both in uplink and downlink hence in GSM radio resource allocation is called symmetric allocation.	While in GPRS it is asymmetric, for example it is possible to allocate time slot only in downlink and not in uplink when user is only downloading some file.
7.	In GSM location area concept is used.	In GPRS routing area concept is used.
8.	In GSM Mobile or UE will be in two states i.e. IDLE and READY.	In GPRS UE will be in three states i.e. IDLE, STANDBY and READY.

- GPRS requires the introduction of two new network elements in the GSM network :

1. Serving GPRS Support Node (SGSN),
2. Gateway GPRS Support Node (GGSN).

3.3.9 Applications of GPRS

1. Email
2. Web based application
3. Fax service
4. Text messages

5. Multimedia
6. File transfer
7. Database access
8. Telemetry
9. Point of sale credit card transactions (especially in a flea market or taxi payment where there is no modem).

3.3.10 Limitations of GPRS

1. Limited cell capacity for all users : Limited radio resources can be deployed. Also voice and GPRS share the same network resources.
2. Lower access speed in reality : Maximum GPRS transmission 172.2 kbps can be with single user over all eight time slots without error protection.
3. No support of GPRS mobile terminate connection for a mobile server.

University Questions

1. *Explain functional architecture of GPRS system. What is the frequency range of uplink and downlink in GPRS netwrok ?* GTU : Winter-11, Marks 7
2. *Applications of GPRS.* GTU : Winter-11, Marks 3
3. *Explain the GPRS system architecture.* GTU : Summer-12, Marks 8
4. *Describe what are the limitations of GPRS ?* GTU : Winter-12, Marks 3
5. *What is the difference between GSM and GPRS ? What are the network elements in GPRS that area different from GSM ? What are the limitations of GPRS.* GTU : Summer-13, Marks 7
6. *Explain call routing in the context of GPRS networks.* GTU : Summer-13, Marks 7
7. *How is data routing done in GPRS ? In what respect is data routing different from voice routing ?* GTU : Summer-13, Marks 7
8. *Limitations of GPRS.* GTU : Winter-13, Marks 7
9. *Explain GPRS operations with its architecture.* GTU : Summer-14, Marks 4
10. *Discuss billing and charging in GPRS network.* GTU : Summer-14, 15, Marks 4
11. *Discuss data services in GPRS. Describe applications suitable for GPRS.* GTU : Winter-14, Summer-15, Marks 7
12. *Explain call routing in the context of GPRS networks.* GTU : Summer-15, Marks 7

3.4 Cordless System

- Citizen band radio is low - frequency, low power shot range personal communication system. Since repeaters are not used, citizen band radio is used for local communications upto few kilometers.
- Citizen band radio operates at 27 MHz and transmitter power is 4 to 12 watts. This much power is enough for minimum interference within the specified range. The maximum allowed channels are limited to 40 to ensure communication without interference. Since it uses half-duplex mode for communication there is only one channel needed for a conversion.
- The transmission is done by using AM which requires less bandwidth than FM. The spacing between the channels is 10 kHz.
- User can scan over the channels and can select any particular channel where interference is less. Any user can scan and listen any channel, there is no privacy.

Disadvantages of CB radio

1. There is no privacy
2. There exist co-channel interference.
3. Suitable for short-distance communication.
4. Since it operates at lower frequency it requires larger antenna.

3.5 Wireless Local Loop (WLL)

- Wireless Local Loop (WLL), is a term for providing wireless connections to stationary or near stationary stations within a small service area.
- WLL is generally targeted at the last mile or from a point in the neighbourhood to the user.

3.5.1 Advantages of Wireless Local Loop

1. Ease of installation as the digging is not required.
2. Quick installation of new links i.e. rapid provisioning.
3. The cost is not dependent on distance up to some limit.
4. Concentration of resources especially at the multiplexer to the high bandwidth backbone.

3.5.2 WLL Architecture

- IS-54 architectural reference model for WLL is shown in Fig. 3.5.1

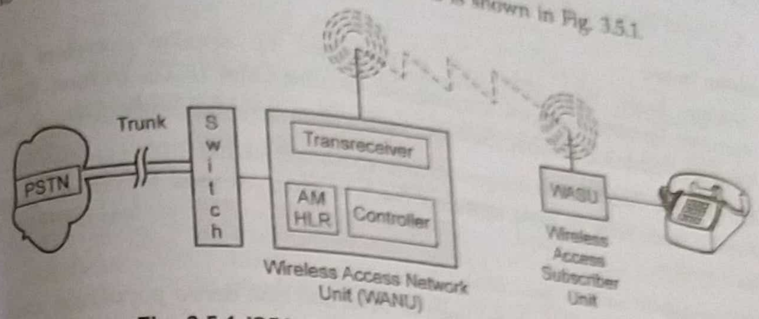


Fig. 3.5.1 IS54 architectural reference model for WLL

3.5.3 WLL Deployment Issues

- Various WLL deployment issues are :

1.Spectrum

- WLL spectrum can be accessed in two modes : licensed and unlicensed band.
- The licensed band spectrum has limited interference, but requires licensing.
- The unlicensed spectrum has more interference, but no licensing is needed. It is generally limited in power.

2.Service quality

- Users expecting service quality should to be the same as wireline telephone service.
- User expects high reliability.
- Every user expects low risk of fraud as there is threat of hijacking the link.

3.Network planning

- The WLL network should support very high penetration levels (for example >90%).
- WLL assumes that users are not moving (or rarely move).
- WLL antenna height is generally derived from user density.

3.5.4 WLL Technologies

- Existing WLL technologies are :
  1. Satellite based
  2. Cellular based

3. Low Tier PCS or Microcellular based

4. Fixed Wireless Access (FWA)

1. Satellite based

- Satellite based WLL technology is supported by satellite operators (Hughes Network Systems, Inmarsat International Circular Orbit (ICO), Iridium, Globestar, Odyssey, American Mobile Satellite Corporation (AMSC), Asia Cellular Satellite (ACeS), Thuraya etc.
- Among these some of these operators (such as Hughes) used terrestrial versions of their system.

2. Cellular based

- Cellular based WLL systems are used in rural and non dense population areas.

3. Low Tier PCS or Microcellular based

- The low tier personal communication systems (PCS) are low power systems. Various low tier PCS are PACS, PHS and DECT etc.

4. Fixed Wireless Access (FWA)

- Fixed wireless accesses are proprietary point-to-point links used for specific areas.

3.6 WiMAX / Wireless Broadband

GTU : Summer-12, Winter-12, 13

- Towards convergence of voice data and video IEEE 802 committee has introduced 802.16 standards for wireless broadband or wireless MAN (Metropolitan Area Network) or Wireless Microwave Access (WiMAX).
- WiMAX is an acronym meaning "Worldwide Interoperability for Microwave Access.
- The IEEE 802.6 standard offers an alternative to high bandwidth wired access networks like fiber optic, cable modems and DSL. It provides network access to buildings through exterior antennas communicating with radio base stations. Networks can be created just by deploying a small number of base stations on buildings to create high capacity wireless access systems.
- In Wireless MAN the traffic movement between subscribers and core network involves following steps:

1. Subscriber sends wireless traffic at speeds ranging from 2M to 155 M bit/sec from a fixed antenna on a building.
2. The base station receives transmissions from multiple sites and sends traffic over wireless or wired links to switching center by using 802.16 protocol.
3. The switching center sends traffic to an Internet Service Provider (ISP) or the public switched telephone network.

Sub-standards of IEEE 802.16

Standard	Description
IEEE 802.16.1	Air interface for 10 to 66 GHz
IEEE 802.16.2	Coexistence of broadband wireless access systems
IEEE 802.16.3	Air interface for licensed frequencies, 2 to 11 GHz

- Different IEEE 802.16 Standards and its scope is summarized in Table 3.6.1

Standard	Scope
IEEE 802.16	Medium access control (MAC) : one common MAC for wireless MAN standards Physical layer : 10 to 66 GHz
IEEE 802.16a	MAC modifications to 802.16.1 Physical layer : 2 to 11 GHz
IEEE 802.16c	Detailed System Profiles for 10-66 GHz
IEEE 802.16e	Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
IEEE 802.16.2	Coexistence of Fixed Broadband Wireless Access Systems

Table 3.6.1

3.6.1 IEEE 802.16 Architecture

- The 802.16 standards are organized into three layer architecture.

1. Physical Layer
2. MAC Layer
3. Convergence Layer

Physical Layer

- Physical layer specifies the frequency band, modulation scheme, and error coding techniques, synchronization between transmitter and receiver data rate and the multiplexing structure.
- Both TDD and FDD alternatives support adaptive bursts profiles in which modulation and coding options may be dynamically assigned on a burst-by-burst basis.

MAC Layer

- The MAC layer is designed for point-to-multipoint broadband access.
- The MAC layer is responsible for transmitting data in frames and controlling access to shared wireless medium.

- The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.
- MAC protocol addresses the need for very high bit rates, both uplink (to base station) and down link (from base station).
- MAC protocol is equipped to accommodate services like multimedia and voice.

Convergence Layer

- Convergence layer provides functions specific to the service being provided.
- For IEEE 802 .16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone networks and frame relay.

University Questions

1. *Differentiate the WiMAX and WiFi technologies.* GTU : Summer-12, Marks 6
2. *What is WiMax ? How is it different from WiFi ?* GTU : Winter-12, Marks 3
3. *Explain WiMax* GTU : Winter-13, Marks 3

3.7 IP and Mobile IP

GTU : Winter-11, Summer-14, 15

3.7.1 Internet Protocol (IP)

- Internet Protocol (IP) is the basic protocol at network layer (L3) which is used for transmission over the Internet.
- IP is designed for use by networks which employ packet-switched data communication. IP provides the connection to the router for transmission
- Each packet is treated independently. Every packet must contain complete destination addressing information.

3.7.2 Mobile IP

- IP stands for Internet Protocol and it works at the third layer of OSI model i.e. Network Layer. The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the internet. Each computer (known as a host) on the internet has at least one IP address that uniquely identifies it from all other computers on the internet.
- The data of a message such as an e-mail note or a Web page, the message gets divided into little chunks called packets. Each of these packets contains both the sender's internet address and the receiver's address.
- Any packet is sent first to a gateway computer that understands a small part of the internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the internet until one gateway recognizes the packet as belonging to a computer within its immediate neighbourhood or domain.
- That gateway then forwards the packet directly to the computer whose address is specified. Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the internet. Packets can arrive in a different order than the order they were sent in.
- The Internet Protocol just delivers them. It's upto another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.
- When user is mobile using laptop with Wi-Fi, the IP address changes with user movement, forcing to terminate connection. This situation of mobility with data connection alive is handled by mobile IP technology.
- The mobile IP signifies that, while a user is connected to applications across the internet and the user's point of attachment changes dynamically, all connections are maintained despite the changes in underlying network properties.
- Mobile IP allows the mobile node to use two IP addresses called home address and care of address. The home address is static and known to everybody as the identity of the host. The care of address changes at each new point of attachment.

3.7.2.1 Working of Mobile IP

- Suppose a mobile node (A) wants to connect to another host (server X). Fig. 3.7.1 Illustrates the working of mobile IP.

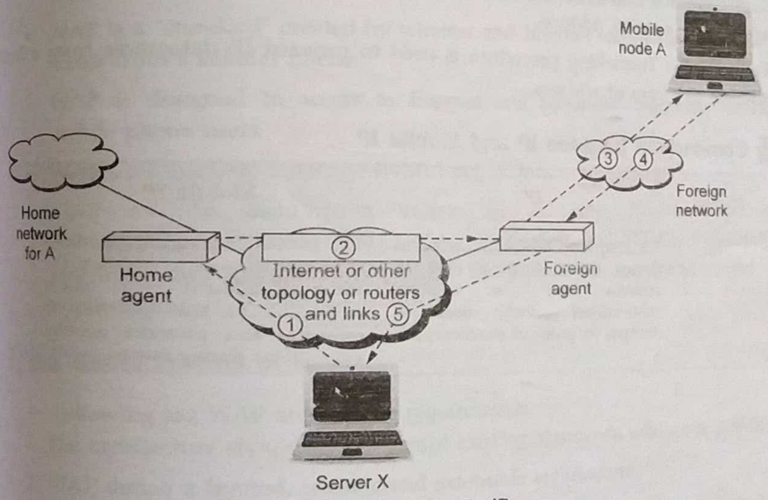


Fig. 3.7.1 Mobile IP

- Host (server X) wants to transmit an IP datagram to mobile node A. The home address of A is known to X. The host X does not know whether A is in home network or any other network. Therefore, host X sends the packet to A with A's home address as the destination IP address in the IP header.
- The IP datagram is routed to A's home network. At A's home network, the incoming IP datagram is intercepted by home agent. The home agent discovers that A is in a foreign network. A care of address is allocated to A by the foreign network and available with the home agent.
- The home agent encapsulates the entire datagram inside a new IP datagram, with A's care of address in the IP header. This new datagram with the care of address as the destination address is retransmitted by the home agent.
- The incoming IP datagram is intercepted by the foreign agent at foreign network. The foreign agent is the counterpart of the home agent in the foreign network.
- The foreign agent strips off the outer IP header, and delivers the original datagram to A. The mobile node A intends to respond to this message and sends traffic to X. The IP datagram from A to X travels directly across the network, using X's IP address as the destination address.

To support the entire operation, the mobile IP should have three basic qualities-

1. **Discovery :** The mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
2. **Registration :** A mobile node uses a registration procedure to inform its home agent of its care-of- address.
3. **Tunnelling :** Tunnelling procedure is used to forward IP datagrams from a home address to a care of address.

3.7.3 Comparison between IP and Mobile IP

Sr. No.	IP	Mobile IP
1	For simple IP protocol, a wireless device must obtain a new IP address (and lose existing connections) every time it changes its point of attachment.	For mobile IP protocol, a wireless device is allowed to maintain the same IP address as it moves from link to link (network to network) and preserve existing connections during moves.
2	Simple IP provides a low level of IP address mobility. Simple IP requires that mobile users remain associated with the same PDSN for mobile nodes to retain the same IP address. As long as the user moves among the cells associated with the PDSN, the PDSN keeps track of the mobile node and assigns it the same IP address each time that it reconnects through a new cell. Simple IP is similar to IP addressing in a wired connection, where one address maps to one connection.	Mobile IP (MIP) provides a higher level of mobility than simple IP. With mobile IP, a subscriber is issued a single IP address for the duration of the session regardless of where they move on the network. The subscriber may roam to another provider's network if a roaming agreement exists, and the subscriber moves outside of the geographic area of the home network.

University Questions

1. *Explain tunneling and encapsulation in mobile IP.* GTU : Winter-11, Marks 7
2. *Compare : IP and Mobile IP.* GTU : Summer-14, Marks 7
3. *How does the Mobile IP work ? Explain its architecture.* GTU : Summer-15, Marks 7

3.8 WAP (Wireless Application Protocol)

GTU : Winter-11,12, Summer-14

- WAP stands for Wireless Application Protocol. WAP is an application communication protocol.WAP is used to access services and information.
- WAP is a "standard" created by wireless and Internet companies to enable Internet access from a cellular phone.
- WAP is designed to access to Internet and advanced telephony services from mobile phone users.
- WAP uses mark-up language (WML) not HTML.
- WAP can be used from variety of 2G and 3G networks such as GSM-900,GSM-1800,GSM-1900,CDMA IS-95,cdma-2000,TDMA IS-136,i-mode,3G systems : IMT-2000,UMTS,W-CDMA. GPRS and 3G are more suited for these applications.

3.8.1 Requirements of WAP

- Following are WAP architecture requirements :

1. The architecture should have leverage existing standards whenever possible.
2. WAP define a layered, scalable and extensible architecture.

3. WAP architecture must support as many wireless networks as possible.

4. Optimization for narrow band bearer with high latency.

5. Optimize for efficient use of device resources.

6. Provide support for secure application and communication.

3.8.2 WAP Protocol Stack

- WAP is designed in a layered fashion so that it can be extensible, flexible and scalable. As a result, the WAP protocol stack is divided into five layers :
  1. Wireless Application Environment (WAE)
  2. Wireless Session Protocol (WSP)
  3. Wireless Transaction Protocol (WTP)
  4. Wireless Transport Layer Security (WTLS)
  5. Wireless Datagram Protocols (WDP)

3.8.2.1 Wireless Application Environment (WAE)

- This layer is of most interest to content developers because it contains, among other things, device specifications and the content development programming languages, WML and WMLScript.
- WAE architecture allows all content and services to be hosted on standard Web servers when all content is located using WWW standard URLs.
- The application environment of WAE consists of :

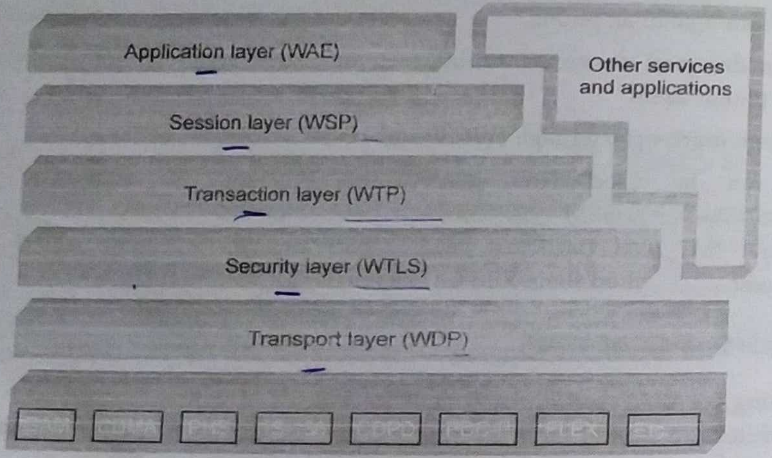


Fig. 3.8.1

1. User agent : Browser or client program
2. WML : Wireless Markup Language is a lightweight markup language optimized for use in wireless devices.
3. WMLScript : Lightweight client side scripting language
4. Wireless Telephony Application : Telephony services and programming interfaces
5. WAP Push Architecture : Mechanism to allow origin servers to deliver content to terminal
6. Content formats : Set of data formats

3.8.2.2 Wireless Session Protocol (WSP)

- Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.
- WSP provides a consistent interface between two session services like client and server.
- WSP offers both connection oriented and connectionless service.

3.8.2.3 Wireless Transaction Protocol (WTP)

- Wireless Transaction Protocol (WTP) runs on top of a datagram service such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.
- WTP supports class of transaction service, optional user-to-user reliability, PDU concatenation and asynchronous transaction.

3.8.2.4 Wireless Transport Layer Security (WTLS)

- WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial and authentication services.
- WTLS provides data integrity, privacy, authentication, denial of service protection.

3.8.2.5 Wireless Datagram Protocol (WDP)

- The WDP is transport layer protocol in WAP architecture. WDP operates above data capable bearer services supported by various network type general transport service.
- The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher

layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

3.8.3 Advantage of WMLScript over WML

- WMLScript provides following advantages to application developer.
  1. Local validation of user input before it is sent to the content server.
  2. Access device resources, functions and peripherals.
  3. Interact with users without reference to origin server.
  4. WMLScript is based on industry standard JavaScript solution.
  5. WMLScript adds power of procedural logic to WML.
  6. WMLScript may be invoked in response to certain event.
  7. WMLScript is fully integrated with the WML browser.

3.8.4 WAP Gateway

- WAP gateway acts as a middleware which performs coding and encoding between cellular device and the web server.
- WAP gateway can be located either in a telecom network or within a computer data network (ISP).
- WAP gateway implements a WAP protocol stack. It performs protocol translation between phone and server.
- WAP gateway compresses WML pages to save bandwidth.
- WAP gateway performs user authentication and billing. Architecture of WAP gateway is shown in Fig. 3.8.2.

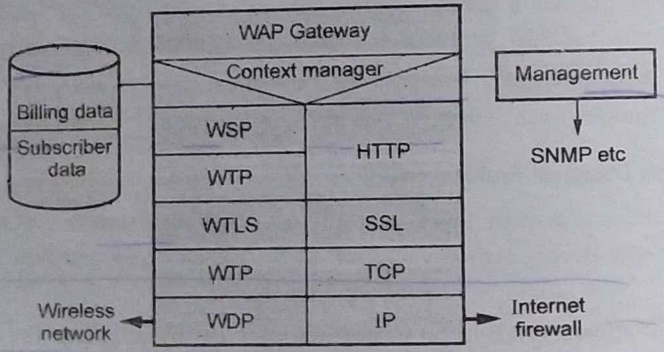


Fig. 3.8.2 WAP gateway architecture

- External interfaces to WAP gateways are :
  - a) SMS center using protocols
  - b) HTTP servers to fetch WML pages
  - c) WAP devices using WAP protocol stack

Functions of WAP Gateway

1. Implementation WAP protocol stack
2. Protocol translation between mobile handset and server
3. Compress WML pages to save bandwidth
4. User authentication and billing

University Questions

1. *State the requirements of WAP and explain different layers of WAP. What are the advantages of WML script over WML ?* **GTU : Winter-11, Marks 4**
2. *What is a WAP gateway ? What are its functions ?* **GTU : Winter-12, Marks 4**
3. *Describe the WAP protocol stack. What are the functions of different layers in this protocol stack ?* **GTU : Winter-12, Marks 7**
4. *Describe the WAP protocol stack while enumerating the functions of different layers.* **GTU : Summer-13, Marks 7**
5. *Explain WAP.* **GTU : Summer-14, Marks 4**

3.9 Multiple Choice Questions

Q.1 GSM provides only _______ data connection.

a 8.6 kbps b 9.6 kbps
c 7.6 kbps d 8.8 kbps [Ans. : b]

Q.2 The uplink and downlink frequencies for GSM are different and therefore a channel has a pair of frequencies _______ apart

a 70 MHz b 80 MHz
c 90 MHz d 60 MHz [Ans. : b]

Q.3 The separation between uplink and downlink frequencies are called _______.

a duplex distance b double distance
c triplex distance d none of these [Ans. : a]

Q.55 The static information is the _______ .

a international mobile subscriber identity

b service subscription information authentication key

c all of these

d account status

[Ans. :d]

Q.56 The dynamic information is the _______ area of the mobile subscriber which is the identity of the currently serving VLR.

a last location

b first location

c current location

d. none of these

[Ans. : c]

Q.57 The HLR handles SS7 transactions with both _______ .

a MSCs

b VLR nodes

c both a & b

d. none of these

[Ans. : c]

Q.58 VLR main tasks are association with _______ .

a MSC

b IMSI

c TMSI

d. roaming

e. all of these

[Ans. : e]

□□□

4 Wi-Fi and the IEEE 802.11 Wireless LAN Standard

Syllabus

IEEE 802 architecture, IEEE 802.11 architecture and services, IEEE 802.11 Medium access control, IEEE 802.11 physical layer, Wi-Fi protected access.

Contents

4.1 IEEE 802 Architecture

- The basic functions of a LAN is organized by set of layering protocols.

802 Protocol Architecture

- Protocols defined specifically for LAN and MAN transmission address issues relating to the transmission of blocks of data over the network
- In OSI terms, higher layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs, MANs, and WANs.
- Fig. 4.1.1 shows relation between LAN protocols to the SI architecture.

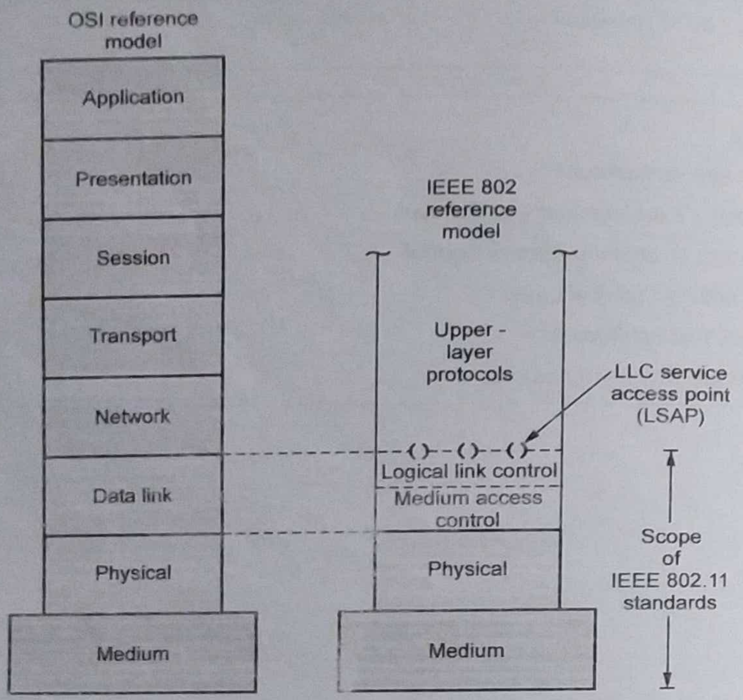


Fig. 4.1.1 IEEE 802 Protocol layers

OSI Layer-1/ Lowest (Physical) Layer Comparison

- The lowest layer of the IEEE 802 reference model corresponds to the physical layer of the OSI model and includes such functions as
  1. Encoding/decoding of signals (e.g., PSK, QAM, etc.)
  2. Preamble generation/removal (for synchronization)
  3. Bit transmission and reception

- The physical layer of the 802 model includes a specification of the transmission medium and the topology. The choice of transmission medium and topology is critical in LAN design, and so a specification of the medium is included.
- Two sublayers are defined in IEEE 802.11.

1. Physical layer convergence procedure (PLCP):

- PLCP defines a method of mapping 802.11 MAC layer protocol data units (MPDUs) into a framing format suitable for sending and receiving user data and management information between two or more stations using the associated PMD sublayer.

2. Physical medium dependent sublayer (PMD):

- PMD defines the characteristics of, and method of transmitting and receiving, user data through a wireless medium between two or more stations.

OSI Layer-2/ Data Link Layer Comparison

- The data link layer is above the physical layer. The functions associated with providing service to LAN users are include-
  1. On transmission- assemble data into a frame with address and error detection fields.
  2. On reception- disassemble frame, and perform address recognition and error detection.
  3. Govern access to the LAN transmission medium.
  4. Provide an interface to higher layers and perform flow and error control.
- The data link layer is divided into two layers-Logical Link Control (LLC) and Media Access Control.
- The above listed first three functions are similar and this specific separate layer is called Medium Access Control (MAC).
- The layer separation is done for the following reasons:
  1. The logic required to manage access to a shared-access medium is not found in traditional layer 2 data link control.
  2. For the same LLC, several MAC options may be provided.

4.2 IEEE802.11 Architecture and Services

- Model developed by the 802.11 working group is shown in Fig. 4.2.1

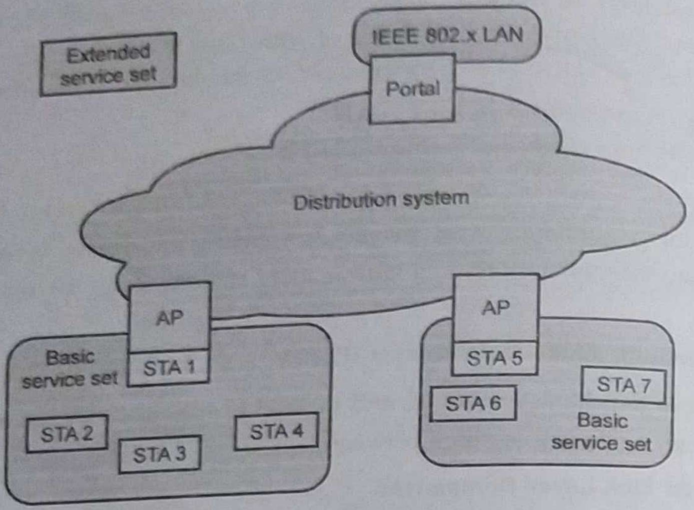


Fig. 4.2.1 IEEE 802.11 architecture

- The smallest building block of a wireless LAN is a basic service set (BSS), which is a set of stations controlled by a single coordination function.
- A BSS may be isolated or it may connect to a backbone distribution system (DS) through an access point (AP). The access point is any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations. The access point functions as a bridge.
- ESS is a set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.

4.2.1 IEEE 802.11 Services

- The IEEE 802.11 defines a set of services that provides the functionality needed to let the LLC layer send and receive MSDUs (MAC Service Data Units).
- The services includes the following : Authentication, deauthentication, privacy, MSDU delivery, association, disassociation, distribution, integration and reassociation.
- Following table shows IEEE802.11 services, provider and the function for which services used to support.

Service	Provided	Used to support
Association	Distribution system	MSDU deliver
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy station	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

- Authentication and deauthentication deals with the station authenticating itself to the network, when joining and leaving the network. Authentication is necessary because the network is wireless which means that it is very easy to eavesdrop.
- The IEEE 802.11 standard defines two kinds of authentication : *Open system authentication* where the station wishing to join the network sends an authentication management frame containing its identification, if the station is known it is accepted otherwise it is not and *Shared key authentication* where a shared secret key has to be known by the station trying to join the network. To use Shared Key Authentication, implementation of the Wired Equivalent Privacy (WEP) algorithm is required.
- Privacy protects the network from eavesdropping. This is necessary because wireless networks are very easy to listen in on, the eavesdropper does not even have to be in the building. Privacy is obtained through the use of the Wired Equivalent Privacy (WEP) algorithm.
- WEP is designed to provide at least the same level of security as wired networks. WEP allows different ciphers to be used as long as a consensus on the network is reached of course. If the wireless network is an ESS, which means that a distribution system is present, additional steps has to be taken. In this case a station has to associate with the access point it is currently using to let the distribution system properly map its location. When the station leaves the access point it will disassociate from the access point.
- The distribution service concerns itself with moving packets from one BSS to another. The distribution has to be aware of the proper destination BSS for the packets that it receives.

- Because the characteristics of the distribution system is unspecified by the IEEE 802.11 standard, integration is needed. This is acquired through the use of a portal that converts IEEE 802.11 packets to the format of the distribution system and back.
- When a station moves from one BSS to another it needs to reassociate in order to receive packets properly. The reassociation service allows a station to change from one access point to another. Reassociation is always initiated by the mobile station.

4.2.2 Comparison of Re-association and Dissociation

Sr. No.	Re-association	Dissociation
1.	The re-association service is used when a MS moves from one BSS to another within the same ESS.	The dissociation service is used to terminate as association.
2.	It is always initiated by the MS.	It may be invoked by either party to an association (the AP or the MS)
3.	It enables the distribution system to recognize the fact that the MS has moved its association from one AP to another.	It is notification and not a request. It cannot be refused. MSs leaving a BSS will send a dissociation message to the AP which need not be always received.

4.3 IEEE 802.11 Medium Access Control

- The IEEE 802.11 MAC layer covers three functional areas :
  1. Reliable data delivery,
  2. Access control, and
  3. Security

4.3.1 Reliable Data Delivery

- A wireless LAN using the IEEE 802.11 physical and MAC layers is subject to unreliable.
- Noise, interference and other propagation effects result in loss of significant no. of frames. This situation can be dealt with by reliability mechanisms at a higher layer, such as TCP.
- For this purpose, IEEE 802.11 includes a frame exchange protocol.
- Frame exchange protocol -
  1. Source station transmits data
  2. Destination responds with acknowledgment (ACK)
  3. If source doesn't receive ACK, it retransmits frame

4.3.2 Access Control

- IEEE 802.11 considered 2 types of MAC algorithm :
  1. Distributed Access protocols
  2. Centralized Access protocols.
- End result for 802.11 is a MAC algorithm called DFWMAC (Distributed Foundation Wireless MAC).
- Fig. 4.3.1 shows IEEE 802.11 Protocol Architecture.

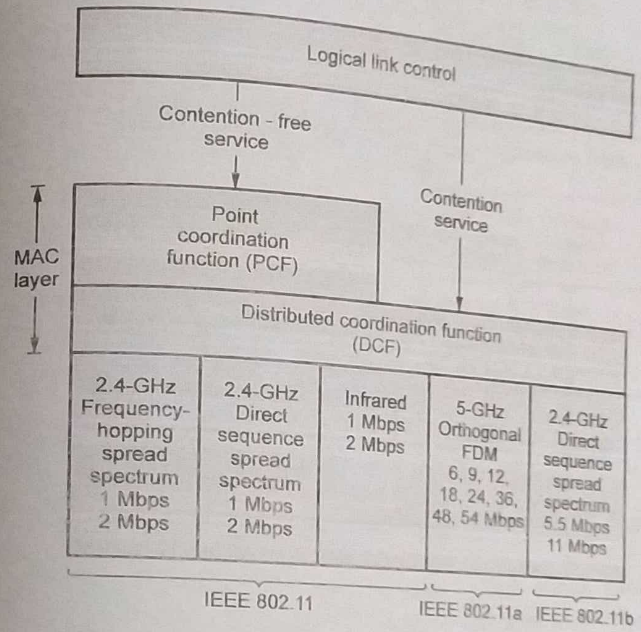

Logical link control
Contention - free service
Contention service
MAC layer
Point coordination function (PCF)
Distributed coordination function (DCF)
2.4-GHz Frequency-hopping spread spectrum 1 Mbps 2 Mbps
2.4-GHz Direct sequence spread spectrum 1 Mbps 2 Mbps
Infrared 1 Mbps 2 Mbps
5-GHz Orthogonal FDM 6, 9, 12, 18, 24, 36, 48, 54 Mbps
2.4-GHz Direct sequence spread spectrum 5.5 Mbps 11 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b

Fig. 4.3.1 IEEE 802.11 architecture

Distributed Coordination Function

- DCF makes use of simple CSMA algorithm.

(a) If a station has MAC frame to transmit, it listens to the medium.

(b) If the medium is idle, station may transmit.

(c) Otherwise it must wait until current transmission is complete.

- DCF does not include a Collision detection function
- To ensure smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme.
- Let us consider a single delay known as an Inter Frame Space (IFS).

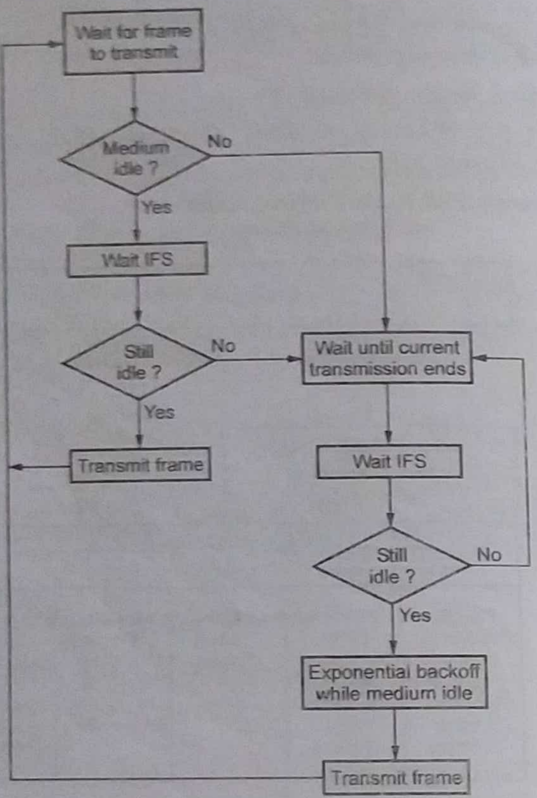

Wait for frame to transmit
Medium idle ?
No
Yes
Wait IFS
Still idle ?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle ?
No
Yes
Exponential backoff while medium idle
Transmit frame

Fig. 4.3.2 IEEE 802.11 Medium Access Control Logic

3. Different Interframe Space (IFS) values

1. **SIFS (Short IFS) :** The shortest IFS, Used for immediate response actions
2. **PIFS (Point Coordination Function IFS) :** A mid-length IFS, used by centralized controller in the PCF scheme.
3. **DIFS (Distributed Coordination Function IFS) :** The longest IFS, used as a minimum delay for asynchronous frames.

Interframe Space (IFS) Usage

1. **SIFS (Short IFS):**

   (a) Acknowledgment (ACK)

   (b) Clear to send (CTS)

   (c) Poll response

2. **PIFS (Point Coordination Function IFS)**

   (a) Used by centralized controller in issuing polls

   (b) Takes precedence over normal contention traffic

3. **DIFS (Distributed Coordination Function IFS):**

   (a) Used for all ordinary asynchronous traffic

4.3.3 MAC Frame

Fig. 4.3.3 shows the general MAC frame format of IEEE 802.11.

2 Octets	2 Octets	6 Octets	6 Octets	6 Octets	2 Octets	6 Octets	0-2312 Octets	4 Octets
Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Frame body	FCS

← MAC Header →

Fig. 4.3.3

Frame control :

- This field carries control information being sent from station to station.

Duration/ID :

- In most frames, this field contains a duration value, depending on the type of frame sent.

Address 1, 2, 3 and 4 :

- The address fields contain different types of addresses, depending on the type of frame being sent. These address types may include the Basic Service Set Identification (BSSID), source address, destination address, transmitting station address, and receiving station address.

Sequence control :

- The sequence control is used for fragmentation numbering to control the sequencing.

Body field :

- This field has a variable length payload and its range is 0-2312 bytes.

Frame Check Sequence (FCS) :

- The MAC layer at the sending station calculates a 32 bits FCS using CRC and place the result in this field.

Security Considerations

- IEEE 802.11 has provisions for authentication and privacy. Two types of authentication supported by IEEE 802.11.
  1. Open system authentication and
  2. Shared key authentication.
- Open system authentication is default authentication scheme. The request frame sends the authentication algorithm ID for open system. The response frame sends the results of request.
- The shared key authentication provides a greater amount of security. The request frame sends the authentication frames ID for the shared key using a 40-bit secret code that is shared between itself and AP. The second station sends a challenge text of 128 bytes. The first station sends encrypted text as the response. The second station sends authentication results.

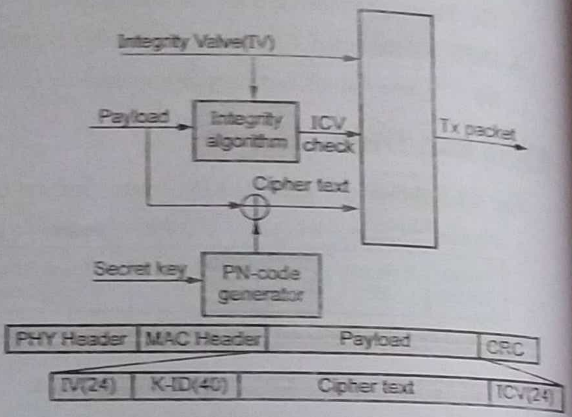


Fig. 4.3.4 Privacy in IEEE 802.11

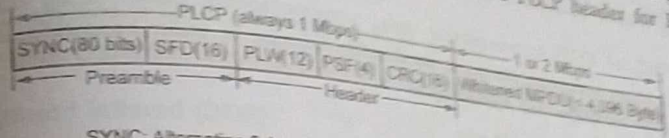
- Privacy is maintained in IEEE 802.11 by Wired-Equivalent Privacy (WEP) specification as shown in Fig. 4.3.4.
- A pseudorandom generator along with 40-bit secret key is used to create a key sequence which is simply a XOR-ed with the plain-text message.

4.4 IEEE 802.11 Physical Layer

- As the MAC Protocol Data Units (MPDU) arrives to PHY Layer Convergence Protocol (PLCP) layer, a header is attached to it, which is designed for PHY medium dependent (PMD) for transmission.
- The PMD transmits the PLCP packet according to specification of signalling techniques.
- Three PLCP packet formats for transmitting PMD are -
  1. FHSS 2. DSSS 3. DFIR

Frequency Hopping Spread Spectrum (FHSS)

- PLCP frame is added to whitened MAC PDU for transmission using FHSS physical specification of IEEE 802.11. Fig. 4.4.1 shows PLCP header for FHSS of IEEE 802.11.



SYNC: Alternating 0.1
SFD: 0000110010111101
PLW: Packet Length Width
PSF: Data rate in 500 kbps steps
CRC: PLCP header coding

Fig. 4.4.1 PLCP header for FHSS of IEEE 802.11

- Two data rates for transmission of information at 1 and 2 Mbps using 2 and four level GFSK modulation respectively.
- The preamble is a sequence of alternating 0 and 1 symbol for 80 bits that is used to extract the received clock for carrier and synchronization.
- The Start of Frame Delimiter (SFD) indicates start of frame and is a specific pattern of 16 bit synchronization.
- The Packet Length Width (PLW) identifies the length of the packet that can be upto 4 kbytes. PLW is of 12 bit length.
- The Packet Signalling Field (PSF) identifies the data rate in 0.5 Mbps steps starting with 1 Mbps. PSF is of 4 bit length.
- The 16-bits CRC code protects the PLCP bits. The overload of PLCP is 128 bits (16 Bytes).
- GFSK modulation technique is used. For 1 Mbps 2 levels and for 2 Mbps 4 levels of GFSK are used.
- Each BSS selects any of the three patterns of 26 hops given by (0, 3, 6, 9....75) or (1, 4, 7, 10........76) or (2, 5, 8, 11......77) as shown in Fig. 4.4.2.

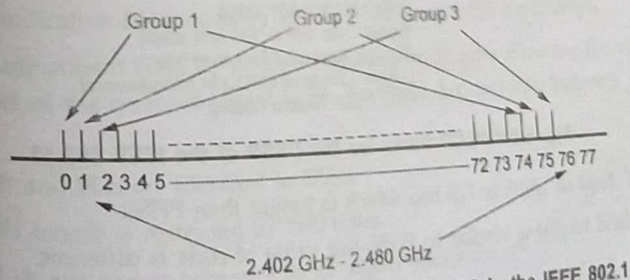


Fig. 4.4.2 Three frequency groups for the FHSS in the IEEE 802.11

- The minimum hop rate of the IEEE 802.11 FHSS system is 2.5 hops per second. The maximum recommended transmitted power is 100 mW.

4.4.2 Direct Sequence Spread Spectrum (DSSS)

- PMD of DSSS communicates using non-overlapping pulses at the chip rate of 11 Mcps occupying 26 MHz bandwidth. Because of wider bandwidth it provides better coverage and stable signal.
- The modulation scheme used for 1 Mbps is DBPSK and for 2 Mbps it is DQPSK which can send 1 or 2 bits per transmitted symbol.
- DSSS implementation requires sampling rate of 11 Mbps.
- The ISM band of 2.4 GHz is divided into 11 overlapping channels spaced by 5 MHz as shown in Fig. 4.4.3 to provide several coexisting channels within a given area.

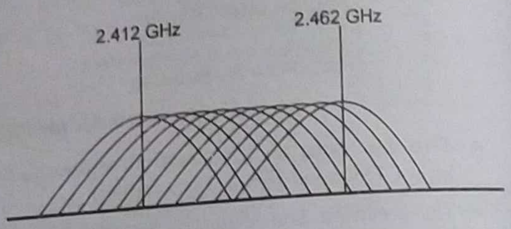
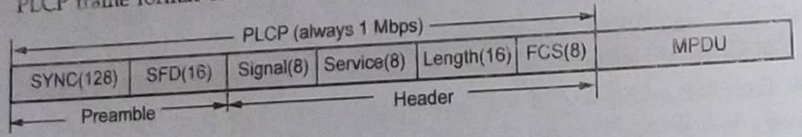


Fig. 4.4.3 Overlapping frequency bands for the DSSS in the IEEE 802.11

- A PHY layer management sublayer of the AP covering a BSS selects one of five choices according to level of interferences.
- PLCP frame format of DSSS version of IEEE 802.11 is shown in Fig. 4.4.4.



SYNC(128)	SFD(16)	Signal(8)	Service(8)	Length(16)	FCS(8)	MPDU

SYNC: Alternating 0,1
SFD: 1111001110100000
Signal: Data rate in 100 kHz steps
Service: Reserved for future use
Length: Length of MPDU in microsecond
FCS: PLCP header coding

Fig. 4.4.4 PLCP frame for the DSSS of the IEEE 802.11

- SYNC field of DSSS is 128 bits which is longer than FHSS.
- SFD field format is similar to FHSS but value of code is different.

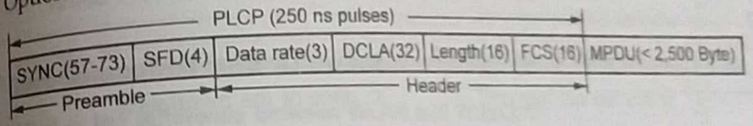
- MPDU does not need to be scrambled for whitening since each bit is transmitted as a set of random chips that is a whitened transmitted signal.
- In DSSS, the service field is reserved for future use. This field is not present in FHSS.
- The length field of DSSS is analogous to PLW of FHSS.
- The Frame Correction Sequence (FCS) field is identical to CRC field of FHSS.

4.4.3 Diffused Infrared (DFIR)

- The PMD of DFIR operates based on transmission of 250 ns pulses generated switching LED.
- Two modulation techniques recommended by IEEE 802.11 -

  Option 1 : 16-PPM for 1 Mbps

  Option 2 : 4 PPM for 2 Mbps



SYNC(57-73)	SFD(4)	Data rate(3)	DCLA(32)	Length(16)	FCS(16)	MPDU(< 2,500 Byte)

SYNC: Alternating 0,1 pulses
SFD: 1001
Data rate: 000 and 001 for
DCLA: DC level adjustments sequences
Length: Length of MPDU in microsecond
FCS: PLCP header coding

Fig. 4.4.5 PLCP frame for the DFIR of the IEEE 802.11

- The peak transmitted power is specified at 2 W with an average of 125 mW or 250 mW. The wavelength of light is at 850 nm to 950 nm.
- PLCP frame format of DFIR version of IEEE 802.11 is shown in Fig. 4.4.5.
- The SYNC and SFD fields are shorter than FHSS and DFSS because non-coherent detection by photosensitive diode detectors does not need carrier recovery.
- Data rate indication field starts by 000 for 1 Mbps and 001 for 2 Mbps.
- DC level adjustment (DLCA) sends a sequence of 32 slots allowing the receiver to set its level of the received signal to set threshold for deciding between zeros and ones.
- The length and FCS are identical to DSSS.
- The MPDU length is restricted to 2500 bytes.
- The DFIR shows higher tolerance to RF signal interference.
- Lower range compare to spread spectrum.

4.4.4 IEEE 802.11a, b

- The PHY layer of IEEE 802.11a is based on OFDM transmission that operates in the 5 GHz U-NII bands same as HIPERLAN-2.
- The OFDM system provides 8 different data rates between 6 to 54 Mbit/s.
- Uses BPSK, QPSK, 16-QAM and 64-QAM modulation schemes coupled with forward error correcting coding.
- Using more power and more efficient data encoding schemes than 802.11b.

4.5 Multiple Choice Questions

Q.1 What is the access point (AP) in wireless LAN ?

a Device that allows wireless devices to connect to a wired network

b Wireless devices itself   c Both (a) and (b)

d None of the mentioned [Ans. : a]

Q.2 In wireless ad-hoc network _____.

a access point is not required   b access point is must

c nodes are not required   d none of the mentioned [Ans. : a]

Q.3 Which multiple access technique is used by IEEE 802.11 standard for wireless LAN ?

a CDMA   b CSMA/CA

c ALOHA   d none of the mentioned [Ans : b]

Q.4 In wireless network an extended service set is a set of _____.

a connected basic service sets

b all stations   c all access points

d none of the mentioned [Ans. : a]

Q.5 IEEE 802.11 have three types of _____.

a frames   b fields   c signals   d sequences [Ans : a]

Q.6 Mostly _______ is used in wireless LAN.

a time division multiplexing

b orthogonal frequency division multiplexing

c space division multiplexing   d none of the mentioned [Ans. : b]

Q.7 DCF stands for _____.

a Direct Control Function   b Distributed Control Function

c Direct Coordination Function   d Distributed Coordination Function [Ans. : d]

Q.8 Which one of the following event is not possible in wireless LAN ?

a Collision detection   b Acknowledgement of data frames

c Multi-mode data transmission   d None of the mentioned [Ans. : a]

Q.9 What is Wired Equivalent Privacy (WEP) ?

a Security algorithm for ethernet   b Security algorithm for wireless networks

c Security algorithm for usb communication

d None of the mentioned [Ans. : b]

Q.10 What is WPA ?

a WI-FI Protected Access   b Wired Protected Access

c Wired Process Access   d WI-FI Process Access [Ans. : a]

4.6 Short Questions and Answers

Q.1 What is the difference between WLAN and WiMAX ?

Ans. : WLAN is used as wireless local area network for providing connectivity between WLAN compliant devices. WiMAX is used as wide area network for providing access between various wireless devices. WLAN standards are evolving including 11a, 11b, 11g, 11n, 11ac, 11ad and more. WiMAX follows IEEE standards viz. 16d and 16e. Both uses OFDM modulation scheme.

Q.2 What is the difference between 802.11a, 11b, 11g and 802.11n ?

Ans. : The difference between the 11a, 11b, 11g and 11n lies in terms of data rate, frequency of operation, distance coverage.

Q.3 What is the difference between WiFi and Bluetooth ?

Ans. : WiFi fall under WLAN category while Bluetooth fall under WPAN category. WLAN specifications are published under IEEE 802.11 and Bluetooth under IEEE 802.15 standards. Bluetooth is the standard for wireless personal area networks or WPAN. It allows high speed transmission of data over very short distances.

Q.4 What is the difference between ad-hoc and infrastructure mode in IEEE 802.11 ?

Ans. : In ad-hoc mode WLAN mobile and stationary terminals referred as STAs (stations) communicate directly. In the infrastructure mode STAs communicate via entity called as AP (Access Point). It is similar to mesh and star topologies used in other wireless networks. Infrastructure mode used to connect with wired network.

□□□

Notes

5 Bluetooth

Syllabus

Radio specification, baseband specification, link manager specification, logical link control and adaption protocol.

Contents

5.1 Bluetooth an Overview GTU : Dec. 2011, May-12, Summer-14, 15, Winter-14

- Bluetooth is an open specification (universal) for short-range wireless voice and data communications. Bluetooth standardization began in 1998.
- Bluetooth is an always-on, short-range radio hook-up that resides on a microchip. It was initially developed by Swedish mobile-phone maker Ericsson in 1994 as a way to let laptop computers make calls over a mobile phone. Since then, several thousand companies have signed on to make Bluetooth the low-power short-range wireless standard for a wide range of devices.
- Sponsors of Bluetooth are : **Initial** : Ericsson, Nokia, IBM, Toshiba and Intel formed a Special Interest Group (SIG) to expand on the concept and to develop a standard under IEEE 802.15 WPAN.
- **Expanded** : In 1999 to include 3 Com, Lucent, Microsoft and Motorola also the first specification, v1.0b was released and then accepted as the IEEE 802.15 WPAN standard for 1 Mb/s networks. Thousands of companies are now adopters of Bluetooth.
- The Bluetooth standards are published by an industry consortium known as the Bluetooth SIG (Special Interest Group).
- The concept behind Bluetooth is to provide a universal short-range wireless capability. It uses the 2.4 GHz band, available globally for unlicensed low-power uses.
- Bluetooth is intended to support an open-ended list of applications including data, audio, graphics, and even video.
- Bluetooth is the first popular technology for short-range ad-hoc networking that is designed for integrated voice and data applications. Compared with WLANs, Bluetooth has a lower data rate, but it has an embedded mechanism to support voice applications.
- Unlike 3G cellular systems, Bluetooth is an inexpensive personal area ad-hoc network operating in unlicensed bands and owned by the user.

Bluetooth Applications

- The bluetooth SIG considers three application-based scenarios :
  1. Cable replacement
  2. Ad-hoc personal networks
  3. Integrated Access Points (APs) for data/voice

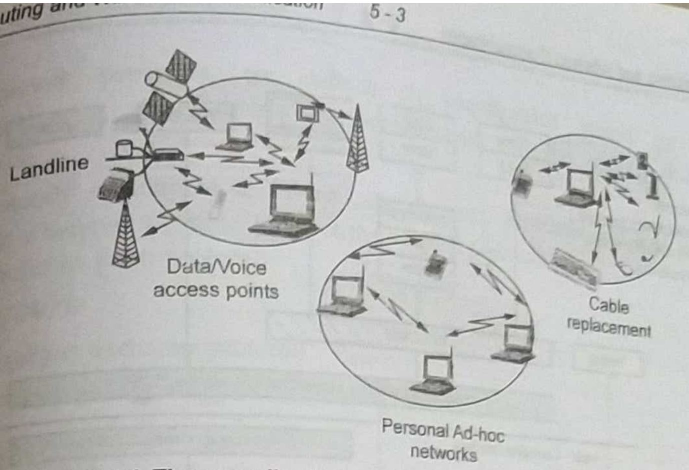


Fig. 5.1.1 Three application scenarios considered by Bluetooth

Bluetooth Standards Documents

- Bluetooth standards are divided into two groups:
  1. **Core Specifications** : Describes the details of the various layers of the Bluetooth protocol architecture, from the radio interface to link control.
  2. **Profile Specifications** : Are concerned with the use of Bluetooth technology to support various applications. Each profile specification discusses the use of the technology defined in the core specifications to implement a particular usage model. It includes a description of which aspects of the core specifications are mandatory, optional, and not applicable.

Protocol Architecture

- Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement, telephony control protocols, and adopted protocols as shown in Fig. 5.1.2 (See Fig. 5.1.2 on next page)
- The core protocols form a five-layer stack consisting of the following blocks:

1. Bluetooth Radio :

- It Specifies the details of the air interface, including frequency, the use of frequency hopping, modulation scheme, and transmit power.

2. BASEBAND :

- It is concerned with connection establishment within a piconet, addressing, packet format, timing, and power control.

3. Link Manager Protocol (LMP) :

- **LMP** is Responsible for linking setup between Bluetooth devices and ongoing link management. (this includes security aspects such as authentication and encryption, plus the control and negotiation of baseband packet sized).

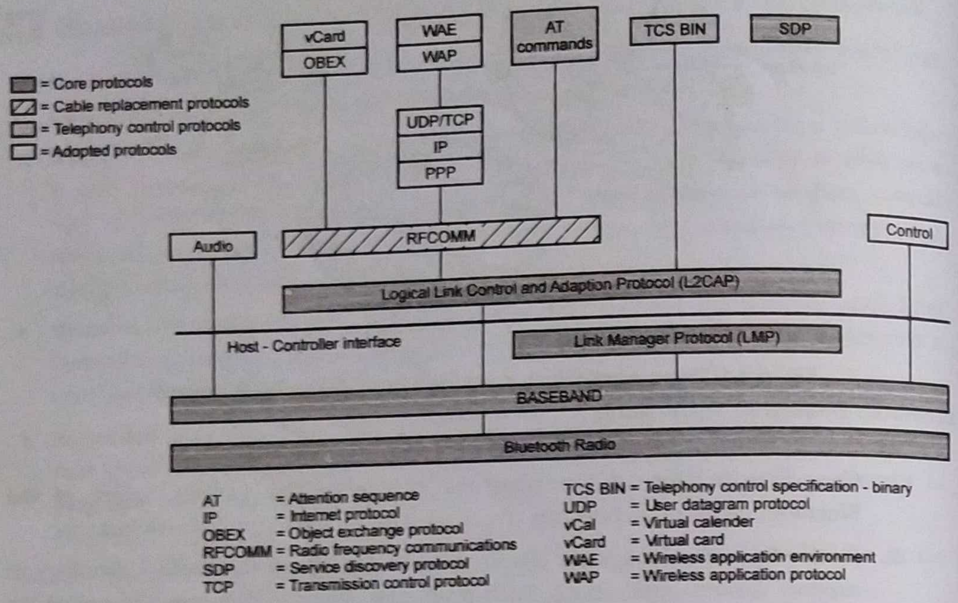

vCard
OBEX
WAE
WAP
AT commands
TCS BIN
SDP
UDP/TCP
IP
PPP
Audio
RFCOMM
Control
Logical Link Control and Adaption Protocol (L2CAP)
Host - Controller interface
Link Manager Protocol (LMP)
BASEBAND
Bluetooth Radio
▆ = Core protocols
▨ = Cable replacement protocols
□ = Telephony control protocols
□ = Adopted protocols
AT = Attention sequence
IP = Internet protocol
OBEX = Object exchange protocol
RFCOMM = Radio frequency communications
SDP = Service discovery protocol
TCP = Transmission control protocol
TCS BIN = Telephony control specification - binary
UDP = User datagram protocol
vCal = Virtual calender
vCard = Virtual card
WAE = Wireless application environment
WAP = Wireless application protocol

Fig. 5.1.2 Bluetooth protocol stack

4. Logical Link Control and Adaptation Protocol (L2CAP) :

- The L2CAP adapts upper-layer protocols to the baseband layer. L2CAP provides both connectionless and connection-oriented services.

5. Service Discovery Protocol (SDP) :

- Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.
- **RFCOMM** is the cable replacement protocol included in the Bluetooth specification. RFCOMM presents a virtual serial port that is designed to make a replacement of cable technologies as transparent as possible.
- RFCOMM provides for binary data transport and emulates EIA-232 control signals over the Bluetooth baseband layer. EIA-232 (formerly known as RS-232) is a widely used serial port interface standard.
- Bluetooth specifies a **telephony control protocol.** TCS BIN (telephony control specification-binary) is a bit oriented protocol that defines the call control signalling for the establishment of speech and data calls between Bluetooth devices.

- The **adopted protocols** are defined in specifications issued by other standards-making organizations and incorporated into the overall Bluetooth architecture.
- The Bluetooth strategy is to invent only necessary protocols and use existing standards whenever possible. Some of the adopted protocols are:

1. PPP (point to point protocol)
2. TCP/UDP/IP
3. OBEX (object exchange protocol)
4. WAE/WAP (wireless application environment and protocol).

University Questions

1. *Explain concept of bluetooth architecture.* GTU : Dec.-11, Marks 4
2. *Explain Service discovery protocol.* GTU : May-12, Marks 2
3. *Explain RFCOMM* GTU : May-12, Marks 2
4. *Explain : Bluetooth* GTU : Summer-14, 15, Marks 4
5. *Explain Bluetooth Protocol Stack.* GTU : Winter-14, Marks 7

5.2 Radio Specification

- The Bluetooth radio specification is a document that gives the basic details of radio transmission for Bluetooth devices. Table 5.2.1 summarizes the key parameters :

Sr No.	Parameter	Typical Value
1.	Topology	Up to 7 simultaneous links in a logical star
2.	Modulation	GFSK
3.	Peak data rate	1 Mbps
4.	RF bandwidth	220 kHz (-3dB), 1 MHz (-20dB)
5.	RF band	2.4 GHz ISM band
6.	RF carriers	23/79
7.	Carrier spacing	1 MHz
8.	Transmit power	0.1 W
9.	Piconet access	FH-TDD-TDMA
10.	Frequency hop rate	1600 hops/s
11.	Scatternet access	FH-CDMA

Table 5.2.1 : Bluetooth Radio and Baseband Parameters.

- Bluetooth makes use of the 2.4 GHz band within the ISM band. In most countries, the bandwidth is sufficient to define 79 1 MHz physical channels.
- Power control is used to keep the devices from emitting any more RF power than necessary. The power control algorithm is implemented using the link management protocol between a master and the slaves in a piconet.
- One important aspect of the radio specifications is the definition of three classes of transmitters based on output power:

I] **Class 1 :** Outputs 100 mW (+20 dBm) for maximum range, with a minimum of 1 mW (0 dBm). In this class power control is mandatory, ranging from 4 to 20 dBm. This mode provides the greatest distance.

II] **Class 2 :** Outputs 2.4 mW (+4 dBm) at maximum, with a minimum of 250 μW (–6 dBm). Powr control is optional.

III] **Class 3 :** Lowest power. Nominal output is 1 mW.

- Modulation for Bluetooth is Gaussian FSK, with a binary one represented by a positive frequency deviation and a binary zero represented by a negative frequency deviation from the centre frequency. The minimum deviation is 115 kHz.

5.2.1 Receiver Characterstics

- The main characteristics of the receivers include the following:

1. **Sensitivity Level :** The receiver must have a sensitivity level for which the bit error rate (BER) 0.1% is met. For Bluetooth this means an actual sensitivity level of –70 dBm or better.
2. **Interference Performance :** The interference performance on Co-channel and adjacent 1 MHz and 2 MHz are measured with the wanted signal 10 dB over the reference sensitivity level. On all other frequencies the wanted signal shall be 3 dB over the reference sensitivity level.
3. **Out-of-Band blocking :** The Out of band blocking is measured with the wanted signal 3 dB over the reference sensitivity level. The interfering signal shall be a continuous wave signal. The BER shall be less than or equal to 0.1%.
4. **Intermodulation Characteristics :** The reference sensitivity performance, BER = 0.1%, shall be met under the following conditions.

a) The wanted signal at frequency f_0 with a power level 6 dB over the reference sensitivity level.

b) A static sine wave signal at f_1 with a power level of –39 dBm.

c) A Bluetooth modulated signal at f_2 with a power level of –39 dBm.

Such that :

$$f_0 = 2 f_1 - f_2 \quad \text{and}$$

$$|f_2 - f_1| = n \cdot 1 \text{ MHz}$$

where n can be 3, 4, or 5. The system must fulfil one of the three alternatives.

5. **RSSI : Receiver Signal Strength Indicator (Optional) :** A transceiver that wishes to take part in a power-controlled link must be able to measure its own receiver signal strength and determine if the transmitter on the other side of the link should increase or decrease its output power level. A Receiver Signal Strength Indicator (RSSI) makes this possible.

- The way the power control is specified is to have a **golden receive power range.** This golden receive power is defined as a range with a lower and higher threshold levels and a high limit.
- The lower threshold level corresponds to a received power between –56 dBm and 6 dB above the actual sensitivity of the receiver.
- The upper threshold level is 20 dB above the lower threshold level to reach an accuracy of ± 6 dB. The instructions to alter the TX power are carried in the LMP link.

5.3 Baseband Specifications

- The Baseband is the physical layer of the Bluetooth. It manages physical channels and links apart from other services like error correction, data whitening, hop selection and Bluetooth security.
- The Baseband layer lies on top of the Bluetooth radio layer in the Bluetooth stack. The baseband protocol is implemented as a Link Controller, which works with the link manager for carrying out link level routines like link connection and power control.
- The baseband also manages asynchronous and synchronous links, handles packets and does paging and inquiry to access and inquire Bluetooth devices in the area.
- The baseband transceiver applies a Time-Division Duplex (TDD) scheme. (alternate transmit and receive). Therefore apart from different hopping frequency (frequency division), the time is also slotted.

5.3.1 Frequency Hopping

- Frequency hopping in Bluetooth serves two purposes :

1. Provides resistance to interference and multipath effects

2. Provides a form of multiple access among co-located devices in different piconets.

- The total bandwidth is divided into 79 **physical channels**, each of bandwidth 1 MHz. FH occurs by jumping from one channel to another in a pseudorandom sequence. The hopping sequence (PN) is shared by all of the devices on a single piconet.
- The hop rate is 1600 hops per second, so that each physical channel is occupied for a duration of 625 μs. Each of the 625 μs time period is referred to as a slot, and these are numbered sequentially.
- Bluetooth radios communicate using a time division duplex discipline (TDD). Because more than two devices share the piconet medium, the access technique is TDMA. Thus, piconet access can be characterized as FH-TDD-TDMA.
- Using TDD prevents crosstalk between the transmit and receive operations in the radio transceiver, which is essential if a one-chip implementation is desired.
- The FH sequence is determined by the master in a piconet and is a function of the master's Bluetooth address. Because different piconets in the same area will have different masters, they will use different hop sequences. Thus, most of the time, transmission on two devices on different piconets in the same area will be on different physical channels.
- Occasionally, two piconets will use the same physical channel during the same time slot, causing a collision and lost data. However, because this will happen infrequently, it is readily accommodated with forward error correction and error detection/ARQ techniques. Thus, a form of CDMA is achieved between devices on different piconets in the same scatternet; this is referred to as FH-CDMA.

5.3.2 Physical Links

- Two types of links can be established between a master and a slave:

1. **Synchronous connection oriented (SCO) :**

- SCO allocates a fixed bandwidth between a point-to-point connection involving the master and a single slave. The master maintains the SCO link by using reversed slots at regular intervals.
- The basic unit of reservation is two consecutive slots (one in each transmission direction). The master can support up to three simultaneous SCO links while a slave can support two or three SCO links. SCO packets are never retransmitted.

2. **Asynchronous connectionless (ACL) :**

- ACL is a point-to-multipoint link between the master and all the slaves in the piconet. In slots not reserved for SCO links, the master can exchange packets with any slave on a per-slot basis, including a slave already engaged in an SCO link.

Only a single ACL link can exists. For most ACL packets, packet retransmission is applied.

5.3.3 Packets

- The packet format for all Bluetooth packets consists of three main fields:

1. **Access Code (72 bits) :** Used for timing synchronization, offset compensation, paging and inquiry.
2. **Header (54 bits) :** Used to identify packet type and to carry protocol control information.
3. **Payload (0 to 2745 bits) :** If present, contains user voice and data and, in most cases, a payload header.

- There are three types of access code :

1. **Channel access code (CAC) :** Identifies the piconet (unique for a piconet).
2. **Device access code (DAC) :** Used for paging and its subsequent responses
3. **Inquiry access code(IAC) :** Used for inquiry purposes.

- The header format for all Bluetooth packets consists of six fields:

1. **AM_ADDR(3 bits) :** Contains the "active mode" address of one of the slaves (there are at most seven devices in a piconet). A transmission from the master to a slave contains that slave's address; a transmission from a slave contains it address. The 0 value is reserved for a broadcast from the master to all slaves in the piconet.
2. **Type :** Identifies the type of packed. Four type codes are reserved for control packets common to both SCO and ACL links. The remaining packet types are used to convey user information.
3. **Flow :** Provides a 1-bit flow control mechanism for ACL traffic only. When a packet with Flow = 0 is received, the station receiving the packet must temporarily halt the transmission of ACL packets on this link. When a packet with Flow = 1 is received, transmission may resume.
4. **ARQN :** Provides 1-bit acknowledgement mechanism for ACL traffic protected by a CRC. If the reception was successful, an ACK (ARQN = 1) is returned; otherwise a NAK (ARQN = 0) is returned. When no return message regarding acknowledge is received, a NAK is assumed implicitly. If a NAK is received, the relevant packet is retransmitted.
5. **SEQN :** Provides a 1-bit sequential numbering schemes. Transmitted packets are alternately labeled with a 1 or 0.
6. **Header Error Control (HEC) :** An 8-bit error detection code used to protect the packet header.

5.3.4 Payload Format

- For some packet types, the baseband specification defines a format for the payload field. For voice payloads, no header is defined. For all of the ACL packets and for the data portion of the SCO packet, a header is defined.
- For data payloads, the payload format consists of three fields :
  1. **Payload header :** An 8-bit header is defined for a single-slot packet, and a 16-bit header is defined for a multi-slot packet.
  2. **Payload body :** Contains user information
  3. **CRC :** A 16-bit CRC code is used on all data payloads except the AUX1 packet (which carries 30 information bytes with no CRC or FEC which is typically used for high-speed data.)
- The payload header, when present consists of three fields:
  1. **L_CH :** Identifies the logical channel.
  2. **Flow :** Used to control flow at the L2CAP level. (This is the same on/off mechanism provided by the flow field in the packet header for ACL traffic).
  3. **Length :** The number of bytes of data in the payload, excluding the payload header and CRC.

5.3.5 Error Correction

- Bluetooth makes use of three error correction schemes:
  a) 1/3 rate FEC
  b) 2/3 rate FEC
  c) ARQ
- These error correction schemes are designed to satisfy competing requirements. The error correction scheme must be adequate to cope with the inherently unreliable wireless link but must also be streamlined and efficient.

5.3.6 Logical Channels

- Bluetooth defines five types of logical data channels designed to carry different types of payload traffic.
  1. **Link Control (LC) :** Used to manage the flow of packets over the link interface. The LC channel is mapped onto the packet header. This channel carries low-level link control information like ARQ, flow control, and payload characterization.
  2. **Link Manage: (LM) :** Transports link management information between participating stations.

3. **User asynchronous (UA) :** Carries asynchronous user data.
4. **User isochronous (UI) :** Carries isochronous user data.
5. **User synchronous (US) :** Carries synchronous user data.

Channel Control

- The operation of a piconet can be understood in terms of the states of operation during link establishment and maintenance.
- There are two major states :
  1. **Standby :** The default state. This is a low-power state in which only the native clock is running.
  2. **Connection :** The device is connected to a piconet as a master or a slave.

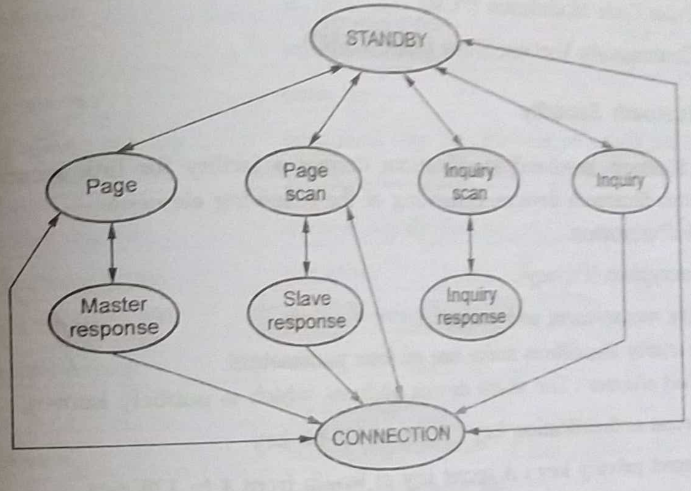


Fig. 5.3.1 Bluetooth state transition diagram

- In addition, there are seven interim sub-states that are used to add new slaves to a piconet. To move from one state to the other, either commands from the Bluetooth link manager or internal signals in the link controller are used. The sub-states are as follows:
  1. **Page :** Used by the master to activate and connect to a slave. Uses the slave device access code (DAC)
  2. **Page scan :** Device is listening for a page with its own DAC.
  3. **Master response :** A device acting as a master receives a page response from a slave. The device can now enter the connection state or return to the page state to page for other slaves.

4. **Slave response :** A device acting as a slave responds to a page from a master. If connection setup succeeds, the device enters the connection state; otherwise it returns to the page scan state.
5. **Inquiry :** Device has issued an inquiry, to find the identity of the devices within range.
6. **Inquiry scan :** Device is listening for an enquiry
7. **Inquiry response :** A device that has issued an inquiry receives an inquiry response.

5.3.8 Bluetooth Audio

- The baseband specifications indicate that either of two voice encoding schemes can be used :
  1. Pulse Code Modulation (PCM)
  2. Continuously Variable Slope Delta (CVSD)

5.3.9 Bluetooth Security

- The Bluetooth baseband specifications defines a facility for link security between any two Bluetooth devices, consisting of the following elements:
  1. Authentication.
  2. Encryption (Privacy).
  3. Key management and usage.
- The security algorithms make use of four parameters:
  1. **Unit address :** The 48-bit device address, which is publicly known.
  2. **Secret authentication key :** A secret 128-bit key
  3. **Secret privacy key :** A secret key of length from 4 to 128 bits
  4. **Random number :** A 128-bit random number derived from a pseudorandom generation algorithm executed in the Bluetooth unit.
- The two secret keys are generated and configured with the unit and not disclosed. The purpose of **authentication** is to verify the claimed identity of one of the two Bluetooth devices involved in an exchange. User information can be protected by **encryption** of the packet payload.

5.4 Link Manager Specifications

GTU : May 2012

- The Link Manager carries out link setup, authentication, link configuration and other protocols. It discovers other remote LM's and communicates with them via

the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).

- The Link Manager Protocol essentially consists of a number of PDU (protocol Data Units), which are sent from one device to another. LM PDUs are always sent as single-slot packets and the payload header is therefore one byte.
- The procedures defined for LMP are grouped into 24 functional areas, each of which involves the exchange of one or more messages. Table 5.4.1 lists these areas, together with the PDUs involved in each area.

Function	PDUs
General response	Accepted, not_accepted
	Security Service
Authentication	au_rand, sres
Pairing	in_rand, au_rand, sres, comb_key, unit_key
Change link key	comb_key
Change current link key	temp_rand, temp_key, use_semi_permanent_key
	Time/synchronization
Clock offset request	clkoffset_req, clkoffset_res
Slot offset information	slot_offset
Timing accuracy	timing_accuracy_req,
Information request	timing_accuracy_res
	Station Capability
LMP version	version_req, version_res
Supported features	features_req, features_res
	Mode Control
Switch master/slave role	switch_req
Name request	name_req, name_res
Detach	detach
Hold mode	hold, hold_req
Sniff mode	sniff, sniff_req, sniff_res
Park mode	park_req, park_set, set_broadcast_window,
	modify_beacon, unpark_PM_ADDR_req,
	unpark_BD_ADDR_req

Power control	incr_power_req, decr_power_req, max_power, min_power
Channel quality-driven	auto_rate, preferred_rate
Change between DM and DH	
Quality of service	quality_of_service, quality_of_service_req
SCO links	SCO_link_req, remove_ SCO_link_req
Control of multi-slot packet	max_slot, max_slot_req
Paging scheme	page_mode_req, page_scan_mode_req
Link supervision	supervision_timeout.

Table 5.4.1 LMP PDUs

University Question

1. *Explain Link manager protocol.* GTU : May-12, Marks 2

5.5 Logical Link Control and Adaptation Protocol (L2CAP)

GTU : May-12

- In the IEEE 802 specification, L2CAP provides a link layer protocol between entities across a shared-medium network. It also provides a number of services and relies on the baseband layer for flow and error control.
- L2CAP makes use of ACL links; it does not provide support for SCO links. L2CAP provides 2 alternatives of service to upper-layer protocols using ACL links:
  1. **Connectionless service :** This is a reliable datagram style of service.
  2. **Connection-mode service :** This is similar to the service offered by HDLC. A logical connection is set up between two users exchanging data. Flow and error control are provided.
- L2CAP provides three types of logical channels :
  1. **Connectionless :** Supports the connectionless service. Each channel is unidirectional and is used for broadcast from the master to multiple slaves.
  2. **Connection-oriented :** Supports connection oriented service. Each channel is full duplex. A quality of service flow specification is assigned in each direction.
  3. **Signalling :** Provides for the exchange of signalling messages between L2CAP entities.

5.5.1 L2CAP Packets

- Fig. 5.5.1 shows the format of L2CAP packets:

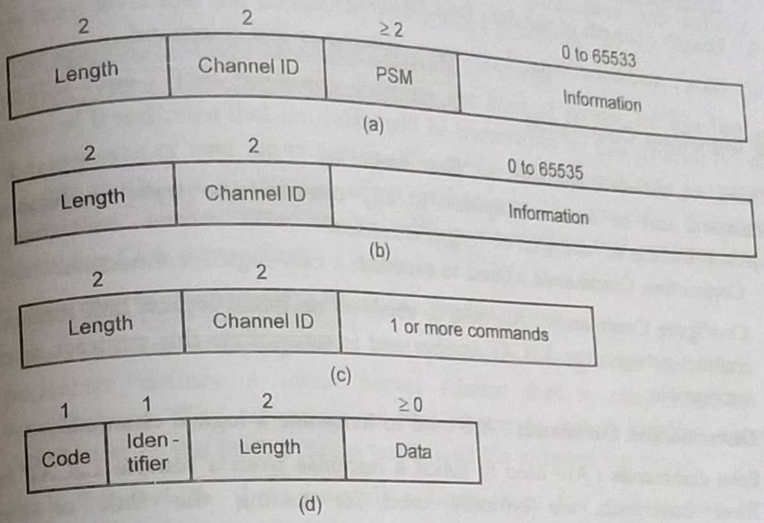


Fig. 5.5.1 L2CAP Packet Format. (a) Connectionless PDU. (b) Connection-oriented PDU. (c) Signalling command PDU. (d) Command Format

- In the connectionless PDU, the following fields are used:
  1. **Length:** Length of the information payload plus PSM fields in bytes
  2. **Channel ID:** A value of 2 indicating the connectionless channel.
  3. **Protocol/Service multiplexer (PSM):** Identifies the higher layer recipient for the payload in this packet.
  4. **Information payload:** Higher layer user data. This field may be up to 65533 bytes in length.
- Connection oriented packets have the same format as connectionless packets, but without the PSM field. The PSM field is not needed because the CID identifies the upper layer recipient of the data. The information payload field may be up to 65535 bytes is length.
- Signalling commands packets have the same header format as the connection-oriented packets. In this case the CID value is 1, indicating the signalling channel. The payload of a signalling packet consists of one or more L2CAP commands, each of which consists of four fields:
  1. **Code :** Identifies the type of command

2. **Identifier :** Used to match a request with its reply. The requesting device sets this field and the responding device uses the same value in its response. A different identifier must be used for each original command.
3. **Length :** Length of the data field for this command in bytes
4. **Data :** Additional data, if necessary, relating to this command.

5.5.2 Signalling Commands

- There are eleven commands in five categories (Table 3). The command reject command can be sent in response to any command to reject it. Reasons for rejection include invalid CID or length exceeded.
  1. **Connection Commands :** Used to establish a new logical connection.
  2. **Configure Commands :** Are sent to establish an initial logical link transmission contract between two L2CAP entities and to renegotiate this contract whenever appropriate.
  3. **Disconnection Commands :** Are used to terminate a logical channel.
  4. **Echo commands :** Are used to solicit a response from a remote L2CAP entity. These commands are typically used for testing the link or passing vendor-specific information using the optional data field.
  5. **Information Commands :** Are used to solicit implementation-specific information from a remote L2CAP entity.

Code	Description	Parameters
0x01	Command reject	Reason
0x02	Connection request	PSM, Source CID
0x03	Connection response	Destination CID, Source CID, Result, Status
0x04	Configure request	Destination CID, Flags, Options
0x05	Configure response	Source CID, Flags, Results, Options
0x06	Disconnection request	Destination CID, Source CID
0x07	Disconnection response	Destination CID, Source CID
0x08	Echo request	Data (optional)
0x09	Echo response	Data (optional)
0x0A	Information request	Info Type
0x0B	Information response	Info Type, Result, Data (optional)

Table 5.5.1 L2CAP signalling command codes.

5.5.3 Quality of Service (QoS)

- The QoS parameter in L2CAP defines a traffic flow specification based on RFC 1363. In essence, a flow specification is a set of parameters that indicate a performance level that the transmitter will attempt to achieve.
- The flow specification consists of the following parameter:
  1. **Service type :** This parameter indicates the level of service for this flow. A value of 0 indicates that no traffic will be transmitted on this channel. A value of 1 indicates a best effort service. The device will transmit data as quick as possible with no guarantees about performance. A value of 2 indicates a guaranteed service (The sender will transmit data that conform to the remaining QoS parameters).
  2. **Token rate (bytes/second) :** See below (bucket size)
  3. **Token bucket size (bytes) :** This parameter, along with the Token rate parameter defines a token bucket scheme that is often used in QoS specifications. The advantage of this scheme is that it provides a concise description of the peak average traffic load the recipient can expect.
  4. **Peak bandwidth (bytes/second) :** Limits how fast packets may be sent back-to-back from applications.
  5. **Latency (microseconds) :** Is the maximum acceptable delay between transmission of a bit by the sender and its initial transmission over the air.
  6. **Delay variation (microseconds) :** Is the difference between the maximum and minimum possible delay that a packet will experience.

University Question

1. *Explain Logical link control and adaptation protocol.* **GTU : May-12, Marks 2**

5.6 Short Questions and Answers

Q.1 What is Bluetooth ?

Ans. : Bluetooth is a wireless technology standard used to exchange data over short distances. The data is exchanged from fixed and mobile devices by creating Personal Area Network with security at high level.

Q.2 What is Piconet ?

Ans. : Piconet is an ad-hoc network by linking a group of users which uses bluetooth technology protocols for allowing one 'master' device to interconnect with up to seven active 'slave' devices. Further, up to 255 slave devices could be inactive or packed and the master device can bring into active status at any given point of time.

Q.6 Unauthorised access of information from a wireless device through a bluetooth connection is called

a bluemaking b bluesnarfing

c bluestring d none of the mentioned [Ans. : b]

Q.7 In the piconet of bluetooth one master device

a can not be slave b can be slave in another piconet

c can be slave in the same piconet d none of the mentioned [Ans. : b]

Q.8 An interconnected collection of piconet is called

a scatternet b micronet

c mininet d none of the mentioned [Ans. : a]

□□□

6 Android

Syllabus

Android APIs, Android Architecture, Application Framework, The Application components, The manifest file, downloading and installing Android, Exploring the Development Environment, Developing and Executing the first Android application, Working with Activities, The LinearLayout Layout, The RelativeLayout Layout, The ScrollView Layout, The TableLayout Layout, The FrameLayout Layout, Using the TextView, EditText View, Button View, RadioButton, CheckBox, ImageButton, RatingBar, The options Menu, The Context Menu.

Contents

6.1 Introduction to Android OS

- Android is an open-source software development platform for creating mobile applications.
- Android is an open source software stack that includes :
  1. Operating system : Linux operating system kernel that provides low level interface with the hardware, memory management and process control.
  2. Middleware : A run time to execute Android applications.
  3. Key mobile applications : Email, SMS, PIM, web browser and etc.
  4. Along with API libraries for writing mobile applications : Including open-source libraries such as SQLite, WebKit and OpenGL ES.
- The components of the underlying OS are written in C or C++, user applications are built for Android in Java. Even the built-in applications are written in Java.
- An important feature of the Android platform is that there's no difference between the built-in applications and applications that is create with the Software Development Kit (SDK).
- Android is only a software. By leveraging its Linux kernel to interface with the hardware, Android runs on many different devices from multiple cell phone manufacturers. Developers write applications in Java.

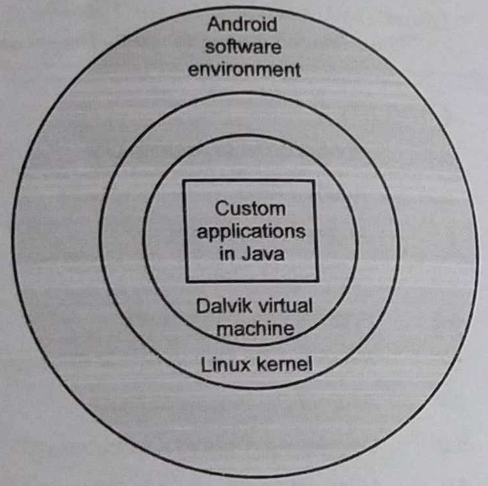


Fig. 6.1.1 Android environment

- The Android software environment and hardware it runs on is shown in Fig. 6.1.1.

6.2 Android APIs

- Android offers a number of APIs for developing your applications. The following list of core APIs should provide an insight into what's available; all Android devices will offer support for at least these APIs :
  1. **android.util** - The core utility package contains low-level classes like specialized containers, string formatters, and XML parsing utilities.

2. **android.os** - The operating system package provides access to basic operating system services like message passing, interprocess communication, clock functions and debugging.
3. **android.graphics** - The graphics API supplies the low-level graphics classes that support canvases, colors and drawing primitives and lets you draw on canvases.
4. **android.text** - The text processing tools for displaying and parsing text.
5. **android.database** - Supplies the low-level classes required for handling cursors when working with databases.
6. **android.content** - The content API is used to manage data access and publishing by providing services for dealing with resources, content providers and packages.
7. **android.view** - Views are the core user interface class. All user interface elements are constructed using a series of Views to provide the user interaction components.
8. **android.widget** - Built on the View package, the widget classes are the "here's one we created earlier" user-interface elements for you to use in your applications. They include lists, buttons and layouts.
9. **com.google.android.maps** - A high-level API that provides access to native map controls that you can use within your application. Includes the MapView control as well as the Overlay and MapController classes used to annotate and control your embedded maps.
10. **android.app** - A high-level package that provides access to the application model. The application package includes the Activity and Service APIs that form the basis for all your Android applications.
11. **android.provider** - To ease developer access to certain standard Content Providers (such as the contacts database), the Provider package offers classes to provide access to standard databases included in all Android distributions.
12. **android.telephony** - The telephony APIs give you the ability to directly interact with the device's phone stack, letting you make, receive and monitor phone calls, phone status and SMS messages.
13. **android.webkit** - The WebKit package features APIs for working with Web-based content, including a WebView control for embedding browsers in your activities and a cookie manager.

6.3 Android Architecture

- Following are the different layers in the Android stack :
  1. Linux kernel layer
  2. Native layer
  3. Application framework layer
  4. Applications layer

  Fig. 6.3.1 illustrates android stack.

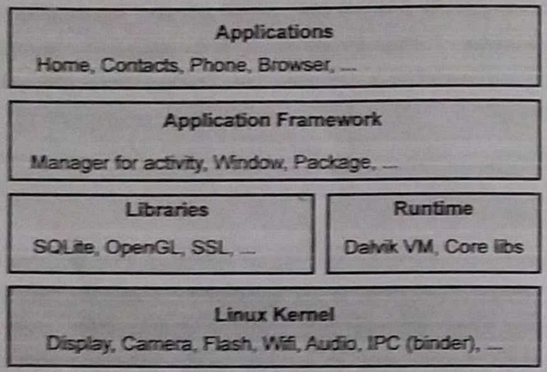

Applications
Home, Contacts, Phone, Browser, ...
Application Framework
Manager for activity, Window, Package, ...
Libraries
SQLite, OpenGL, SSL, ...
Runtime
Dalvik VM, Core libs
Linux Kernel
Display, Camera, Flash, Wifi, Audio, IPC (binder), ...

Fig. 6.3.1 Android stack

1. The Linux kernel layer

- The Linux kernel includes drivers for hardware, networking, file system access and inter-process-communication.
- The Linux kernel is at the bottom of the Android stack. It never really interacts with the users and developers, but is at the heart of the whole system. Its importance stems from the fact that it provides the following functions in the Android system :
  a) Hardware abstraction
  b) Memory management programs
  c) Security settings
  d) Power management software
  e) Other hardware drivers (Drivers are programs that control hardware devices.)
  f) Support for shared libraries
  g) Network stack

2. Native code libraries layer

- The next layer in the Android architecture includes **Android's native libraries.** Libraries carry a set of instructions to guide the device in handling different types of data. For instance, the playback and recording of various audio and video formats is guided by the media framework library.
- The native libraries includes daemons and services (written in C or C++) like browser technology from WebKit, database support via SQLite, advanced graphics support (2D, 3D and animation from scalable games language), audio and video media support from PacketVideo's OpenCORE.

Android Runtime

- The Android runtime are written in Java and executing in Dalvik. The core Java packages used for a full-featured Java programming environment and the Dalvik VM, employs services of the Linux-based kernel to provide an environment to host Android applications.
- Dalvik is open-source software. It is the software responsible for running apps on Android devices.

3. Application framework layer

- An important block of application framework is application manager. The application managers include windows, contents, activities, telephony, location and notifications.

4. Application layer

- The applications are at the topmost layer of the Android stack. An average user of the Android device would mostly interact with this layer (for basic functions, such as making phone calls, accessing the Web browser etc.).
- The layers further down are accessed mostly by developers, programmers and the likes.
- Several standard applications come installed with every device, such as :
  a) SMS client app
  b) Dialer
  c) Web browser
  d) Contact manager

6.4 Application Framework

- **Application Framework** : The application framework provides the classes used to create Android applications. It also provides a generic abstraction for hardware access and manages the user interface and application resources.

- The Android application framework provides everything necessary to implement your average application. The Android application lifecycle involves the following key components :
  1. **Activity Manager** - Controls all aspects of the application lifecycle and activity stack.
  2. **Content Providers** - Allows applications to publish and share data with other applications.
  3. **Resource Manager** - Provides access to non-code embedded resources such as strings, color settings and user interface layouts.
  4. **Notifications Manager** - Allows applications to display alerts and notifications to the user.
  5. **View System** - An extensible set of views used to create application user interfaces.
- The Android application framework includes traditional programming constructs, such as threads and processes and specially designed data structures to encapsulate objects commonly used in mobile applications. Developers can rely on familiar class libraries, such as **java.net** and **java.text**. Specialty libraries for tasks such as graphics and database.
- Android applications can interact with the operating system and underlying hardware using a collection of managers. Each manager is responsible for keeping the state of some underlying system service. For example, there is a **LocationManager** that facilitates interaction with the location-based services available on the handset. The **ViewManager** and **WindowManager** manage user interface fundamentals. Applications can interact with one another by using or acting as a **ContentProvider**.
- Built-in applications such as the Contact manager are content providers, allowing third party applications to access contact data and use it in an infinite number of ways. The sky is the limit.

6.5 Application Components

- Application components are the essential building blocks of an Android application. These components are loosely coupled by the application manifest file *AndroidManifest.xml* that describes each component of the application and how they interact.

- There are following four main components that can be used within an Android application :

Components	Description
Activities	They dictate the UI and handle the user interaction to the smart phone screen
Services	They handle background processing associated with an application.
Broadcast Receivers	They handle communication between Android OS and applications.
Content Providers	They handle data and database management issues.

6.5.1 Manifest File

- Every application must have an **AndroidManifest.xml** file (with precisely that name) in its root directory. The manifest presents essential information about the application to the Android system, information the system must have before it can run any of the application's code. Among other things, the manifest does the following :
  1. It names the Java package for the application. The package name serves as a unique identifier for the application.
  2. It describes the components of the application - the activities, services, broadcast receivers, and content providers that the application is composed of. It names the classes that implement each of the components and publishes their capabilities (for example, which Intent messages they can handle). These declarations let the Android system know what the components are and under what conditions they can be launched.
  3. It determines which processes will host application components.
  4. It declares which permissions the application must have in order to access protected parts of the API and interact with other applications.
  5. It also declares the permissions that others are required to have in order to interact with the application's components.
  6. It lists the Instrumentation classes that provide profiling and other information as the application is running. These declarations are present in the manifest only while the application is being developed and tested; they're removed before the application is published.
  7. It declares the minimum level of the Android API that the application requires.
  8. It lists the libraries that the application must be linked against.

6.5.2 Downloading and Installing Android

- To write Android applications, one must configure programming environment for Java development. The software is available online for download at no cost. Android applications can be developed on Windows, Macintosh, or Linux systems.
- To develop Android applications, you need to have the following software installed on computer :

1. The Java Development Kit (JDK) Version 5 or 6, available for download at

   http://java.sun.com/javase/downloads/index.jsp.

2. A compatible **Java IDE such as Eclipse** along with its JDT plug-in, available for download at http://www.eclipse.org/downloads/.
3. The **Android SDK**, tools and documentation, available for download at

   http://developer.android.com/sdk/index.html.

4. The **Android Development Tools** (ADT) plug-in for Eclipse, available for download through the Eclipse software update mechanism. For instructions on how to install this plug-in, see http://developer.android.com/sdk/eclipse-adt.html.

- Although this tool is optional for development, but it is highly recommend to install it.
- The Android SDK comes with five major components : the Android SDK License Agreement, the Android Documentation, Application Framework, Tools and Sample Applications.

6.6 Exploring the Development Environment

- Developers have several choices when it comes to integrated development environments (IDEs). Many developers choose the popular and freely available Eclipse IDE to design and develop Android applications.
- Eclipse is the most popular IDE for Android development, and there is an Android plug-in available for facilitating Android development.
- Android applications can be developed on the following operating systems :
- Windows XP (32-bit) or Vista (32-bit or 64-bit)
- Mac OS X 10.5.8 or later (x86 only)
- Linux (tested on Linux Ubuntu 8.04 LTS, Hardy Heron)
- Most developers use the popular Eclipse Integrated Development Environment (IDE) for Android development. The Android development team has integrated the Android development tools directly into the Eclipse IDE. However, developers are not constrained to using Eclipse; they can also use other IDEs.

6.7 Android Development Tools

- Various Android development tools are :

6.7.1 Android SDK

- The Android Software Development Kit (Android SDK) contains the necessary tools to create, compile and package Android applications. Most of these tools are command line based.
- The primary way to develop Android applications is based on the Java programming language.
- Android SDK can be freely downloaded from Android website.

6.7.2 Android Debug Bridge (ADB)

- The Android SDK contains the Android Debug Bridge (ADB), which is a tool that allows you to connect to a virtual or real Android device, for the purpose of managing the device or debugging your application.

6.7.3 Android Developer Tools and Android Studio

- Google provides two Integrated Development Environments (IDEs) to develop new applications.
- The Android Developer Tools (ADT) are based on the Eclipse IDE. ADT is a set of components (plug-ins), which extend the Eclipse IDE with Android development capabilities.
- Google also supports an IDE called Android Studio for creating Android applications. This IDE is based on the IntelliJ IDE.
- Both IDEs contain all required functionality to create, compile, debug and deploy Android applications. They also allow the developer to create and start virtual Android devices for testing.

6.7.4 Dalvik Virtual Machine (DVM)

- Android uses the Dalvik virtual machine with just-in-time compilation to run Dalvik byte code, which is usually translated from Java byte code.
- According to Google's Android documentation, the Dalvik VM is an interpreter-only virtual machine that executes files in the Dalvik Executable (.dex) format, a format that is optimized for efficient storage and memory-mappable execution.

- The virtual machine is register-based and it can run classes compiled by a Java language compiler that have been transformed into its native format.
- Currently Android versions use the Dalvik virtual machine. The latest Android versions introduced a new runtime the Android RunTime.

6.7.5 Android RunTime (ART)

- With Android 4.4, Google introduced the Android RunTime (ART) as optional runtime for Android 4.4. It is uses as default runtime for all Android versions after 4.4.
- ART uses Ahead of Time compilation. During the deployment process of an application on an Android device, the application code is translated into machine code. This result in approximately 30 % larger compiles code, but allows faster execution from the beginning of the application.
- This also saves battery life, as the compilation is only done once, during the first start of the application.
- The **dex2oat** tool takes the .dex file created by the Android tool change and compiles that into an Executable and Linkable Format (ELF file). This file contains the dex code, compiled native code and meta-data. Keeping the .dex code allows that existing tools still work.
- The garbage collection in ART has been optimized to reduce times in which the application freezes.

6.8 Developing Android Applications

- Android applications are primarily written in the Java programming language.
- During development the developer creates the Android specific configuration files and writes the application logic in the Java programming language.
- The ADT or the Android studio tools convert these application files, transparently to the user, into an Android application.
- When developers trigger the deployment in their IDE, the whole Android application is compiled, packaged, deployed and started.

6.8.1 Conversion Process from Source Code to Android Application

- The Java source files are converted to Java class files by the Java compiler.
- The Android SDK contains a tool called dx which converts Java class files into a *.dex* (Dalvik Executable) file. All class files of the application are placed in this *.dex* file.

- During this conversion process redundant information in the class files are optimized in the *.dex* file.For example, if the same **String** is found in different class files, the *.dex* file contains only one reference of this **String**.
- These *.dex* files are therefore much smaller in size than the corresponding class files.
- The *.dex* file and the resources of an Android project, e.g., the images and XML files, are packed into an *.apk* (Android package) file. The program *aapt* (Android Asset Packaging Tool) performs this step.
- The resulting *.apk* file contains all necessary data to run the Android application and can be deployed to an Android device via the *adb* tool.

6.8.2 Android SDK Features

- Important features of Android SDK are as under.

1. No licensing, distributions or development fees or release approval processes.
2. Full multimedia hardware control.
3. APIs for using sensor hardware including accelerometer and the compass.
4. APIs for location based services.
5. Android Inter-Process Communication (IPC).
6. Shared data storage.
7. Background applications and processes.
8. Home screen widgets, live folders.
9. HTML5 WebKit-based web browser.
10. GSM, EDGE and 3G networks for telephony and data transfer.
11. The Android SDK includes development tools which helps compile and debug any app.
12. Android emulator shows how app will look and behaviour on a real Android device.

6.9 Mapping Applications to Processes

- Android relies on Linux for process management and the application itself runs in an instance of the Dalvik VM.
- The OS might need to unload or even kill, an application from time to time to accommodate resource allocation demands.
- The system uses a hierarchy or sequence to select the victim during shortage of resources.

- The rules followed by system are :
  1. Visible or running activities will be given top priority.
  2. Visible, non-running activities are important, because they're recently paused and are likely to be resumed shortly.
  3. Next priority is for running services.
  4. The most likely termination processes are the processes that are empty (loaded perhaps for performance-caching purposes) or processes that have dormant activities.

6.10 Managing of App

6.10.1 Performance of App

- Performance of app plays important role in getting 5 star rating in all marketplaces like playstore, app store or windows store.
- If application takes more than 10 seconds to load then it will not be used by users.
- If application takes too long time to process data then it will not be used by users.
- If application takes too long time to switch between screens then it will not be used by users.
- The performance of app is important factor which decides the success of app.

Improving Performance of App

- Understand your target device. Most developers forget about device, they classify device based on operating system, but forget about configuration of devices. Always classify devices based on specification sheet. Try developing apps based on low specification mobile which will automatically run in all mobiles.
- Understand your tools. Try to understand the tools that are used to develop the mobile app. Better understanding of tools helps to make important architectural design. Example - Understanding about phone gap helps to develop app for multiple platforms.
- Understand core concepts of the language used to build app. Understanding core programming language used to develop app will help to avoid performance issues. Example - A extra string comparison in jscript will surely reduce the performance.
- Understand the library. Try to understand the library used in tools. If you simply call third party methods for simple operation then it will increase battery usage and reduce the performance. Always use standard codes for simple task.

6.10.2 Modifiability of App

- Modifiability helps to release multiple version of app more easily.
- Modifiability is achieved by developing as multiple units instead of single unit.
- If any bugs arise after launch then it is easy to modify the unit instead of changing everything in code.
- Modifiability is minimizing the technical risks and cost impact of changes in software.
- In order to achieve modifiability as a system quality, software architects need to envision and incorporate modifiability support in the system's design cycle.
- The architectural design supports the modifiability requirements of a system.
- The modifiability quality of a system can be expressed in terms of cohesion and coupling. Coupling measures the mutual association strength between the system's software components. Where cohesion, on the other hand, is a measure for the number of internal relationships between the responsibilities of a software component.

6.10.3 Availability of App

- Availability refers to continuous working of application in both offline and in online mode.
- Today mobile users are travelling across multiple cell sites which frequently disturb the wireless internet connectivity to mobile.
- This interruption should not affect the mobile app. It is possible to achieve high availability by effectively managing offline data. High availability can be provided by giving effective synchronization mechanism.

6.10.4 Security

- Mobile apps should satisfy stringent requirements for data security and privacy. This is no longer the exclusive domain of the enterprise : Organizations of every size and function are subject to mounting ethical and legal pressure to control and protect the information under their purview.
- Fiduciary responsibility and internal and external policies exist to govern what organizations must do in this regard, from data storage to disaster recovery, encryption to secure updating.
- By definition, internet access and mobile devices carry inherent security risks, including but not limited to the apps that run on them.

6.11 Layouts

- Layout Managers (more generally, "layouts") are extensions of the ViewGroup class designed to control the position of child controls on a screen.
- Layouts can be nested, letting you create arbitrarily complex interfaces using a combination of Layout Managers.
- The Android SDK includes some simple layouts to help you construct your UI. It's up to you to select the right combination of layouts to make your interface easy to understand and use.
- The following list includes some of the more versatile layout classes available :

1. **FrameLayout**

- The simplest of the Layout Managers, the Frame Layout simply pins each child view to the top left corner. Adding multiple children stacks each new child on top of the previous, with each new View obscuring the last.

2. **LinearLayout**

- A Linear Layout adds each child View in a straight line, either vertically or horizontally. A vertical layout has one child View per row, while a horizontal layout has a single row of Views.
- The Linear Layout Manager allows you to specify a "weight" for each child View that controls the relative size of each within the available space.

3. **RelativeLayout**

- Using the Relative Layout, you can define the positions of each of the child.
- Views relative to each other and the screen boundaries.

4. **TableLayout**

- The Table Layout lets you lay out Views using a grid of rows and columns. Tables can span multiple rows and columns and columns can be set to shrink or grow.

5. **AbsoluteLayout**

- In an Absolute Layout, each child View's position is defined in absolute coordinates. Using this class, you can guarantee the exact layout of your components, but at a price. Compared to the previous managers, describing a layout in absolute terms means that your layout can't dynamically adjust for different screen resolutions and orientations.

6.11.1 Working with Layouts

- Much as web designers use HTML, user interface designers can use XML to define Android application screen elements and layout.
- A layout XML resource is where many different resources come together to form the definition of an Android application screen.

- Layout resource files are included in the /res/layout/ directory and are compiled into the application package at build time. Layout files might include many user interface controls and define the layout for an entire screen or describe custom controls used in other layouts.

6.12 Toolbox

- Android supplies a toolbox of standard Views to help you create simple interfaces. By using these controls (and modifying or extending them as necessary), you can simplify your development and provide consistency between applications.
- The following list highlights some of the more familiar toolbox controls :

1. **TextView**

- A standard read only text label. It supports multiline display, string formatting and automatic word wrapping.

2. **EditText**

- An editable text entry box. It accepts multiline entry and word wrapping.

3. **ListView**

- A View Group that creates and manages a group of Views used to display the items in a list. The standard ListView displays the string value of an array of objects using a Text View for each item.

4. **Spinner**

- Composite control that displays a TextView and an associated ListView that lets you select an item from a list to display in the textbox. It's made from a Text View displaying the current selection, combined with a button that displays a selection dialog when pressed.

5. **Button**

- Standard push-button

6. **CheckBox**

- Two-state button represented with a checked or unchecked box

7. **RadioButton**

- Two-state grouped buttons. Presents the user with a number of binary options of which only one can be selected at a time.

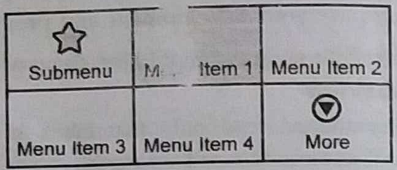
6.13 Menus

- Menus offer a way to expose application functions without sacrificing valuable screen space. Each activity can specify its own activity menu that's displayed when the device's menu button is pressed.
- Android also supports context menus that can be assigned to any View within an Activity. A View's context menu is triggered when a user holds the middle D-pad

button, depresses the trackball or longpresses the touch screen for around 3 seconds when the View has focus.

- Activity and context menus support submenus, checkboxes, radio buttons, shortcut keys and icons.
- To improve the usability of application menus, Android features a three-stage menu system optimized for small screens :

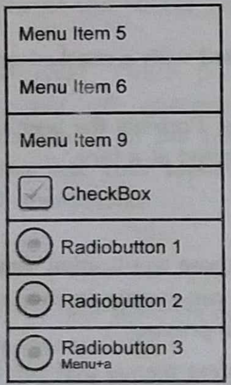
1. The Icon Menu



- This compact menu appears along the bottom of the screen when the Menu button is pressed. It displays the icons and text for up to six Menu Items (or submenus).
- This icon menu does not display checkboxes, radio buttons or the shortcut keys for Menu Items, so it's generally good practice not to assign checkboxes or radio buttons to icon menu items, as they will not be available. If more than six Menu Items have been defined, a More item is included that, when selected, displays the expanded menu. Pressing the Back button closes the icon menu.

2. The Expanded Menu

- The expanded menu is triggered when a user selects the **More** Menu Item from the icon menu. The expanded menu displays a scrollable list of only the Menu Items that weren't visible in the icon menu. This menu displays full text, shortcut keys and checkboxes/radio buttons as appropriate.



3. Submenus

- The traditional "expanding hierarchical tree" can be awkward to navigate using a mouse, so it's no surprise that this metaphor is particularly ill-suited for use on mobile devices.
- The Android alternative is to display each submenu in a floating window. For example, when a user selects a submenu such as the creatively labeled Submenu from menus, its items are displayed in a floating menu Dialog box, as shown in Fig. 6.13.1.

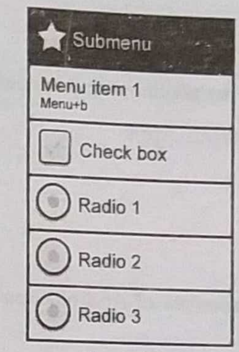


Fig. 6.13.1

6.14 Multiple Choice Questions

Q.1 What is Android ?

a Android is a stack of software's for mobility

b Google mobile device name

c Virtual machine

d None of the above **[Ans. : a]**

Explanation : Android is a stack of software applications for mobile devices, which includes an operating system, middleware applications and some key applications. It executes within own process and own instance of Dalvik Virtual Machine. DVM executes byte code and later transforms into .dex format files.

Q.2 What are the layouts available in android ?

a Linear Layout b Frame Layout

c Table Layout d Relative Layout

e All of above **[Ans. : e]**

Explanation : Android is having Linear Layout(Horizontal and Vertical), Frame Layout, Table Layout and Relative Layout.