RBA

MC module - 1

Total - 15m

1) What is mobile computing ? and explain its components ? (5m)

2) Explain telecommunication generation (10m)
difference for (5m / 10m)

3) What is cellular system (5m)

4) Explain Electromagnetic Spectrum with its application (10m)

5) Explain Antenna with its type (10m)

6) Explain signal propagation and its problem (10m)

7) Define Signal with characteristics (5m / 10m)

8) Explain multiplexing and its types. (10m)

9) What is Spread Spectrum and explain types of it. (DSSS, FHSS) (10m)
slow fast
Any 1 for 5m

Page No.
Date

Module-2

1) Explain Gsm mobile services. (5m)

2) Explain GSM architecture (10m)

3) Explain Radio interfaces used in Gsm (5m)

4) Explain Gsm protocol Stack (10m)

5) Explain localization and calling procers.
(17 step) (10 step)
(10m)

6) Explain handover and types of it (5m)

7) Explain Gsm Security algorithm
(A3, A5, A8)

8) Explain GPRS System architecture (10m)

9) Explain GPRS protocol Stack (10m)

10) Explain UTRAN System architecture. (5m/10m)

i) Mobile computing :

Mobile computing is a technology that allows transmission of data, voice & video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

→ The main concept involves -

i) Mobile communication
ii) Mobile hardware
iii) Mobile software

or

i) → Mobile computing :

A technology that is capable of providing an environment which enables users to transmit data from one device to other device without the use of any physical link / cables is known as mobile computing.

- It means data transmission is done wirelessly with the help of wireless device such as mobiles, laptops etc.
- Mobile computing technology helps users to access & transmit data from any remote location without being present there physically.

Mobile communication

- Mobile communication is the framework i.e. responsible for the working of computing technology.

Components of mobile computing :-

A mobile computing system consist of following components.

i) Mobile Hardware -

→ Mobile Hlw is a small & portable computing device with the ability to retrieve & process data.

→ Smartphone, handheld & wearable devices fall under mobile hlw.

ii) Mobile software -

→ Mobile slw is the slw program which is developed specifically to be run on mobile hlw. This is usually the os in mobile devices

→ These os provides features such as touchscreen cellular connectivity, bluetooth, wi-fi, GPS, camera and sensor.

iii) mobile comm^n -

→ Mobile comm^n refers to the exchange of data & voice using existing wireless networks

Difference between 1G, 2G, 2.5G, 3G, 4G

	Basic Terms	1G	2G	2.5G	3G	4G
1)	Full form	1st generation	Second gen"	Second & Half" gen"	Third gen"	Fourth gen"
2)	Year	1980s	1990s (1991)	2001 - 2003	2005	released in 2008 working fully upto 2009
3)	Support	voice only	sms, picture msg & mms	WAP, mms sms, mobile games & search & directory	digital GPS, video on demand video conferencing	voice, video call mail VOIP internet, Video Streaming
4)	Speed	2.4 kbps	40 - 50 kbps 500 kbps - 1 mbps	20 - 40 kbps 236.8 kbps - 384	2 mbps for non moving devices 384 kbps in moving Vehicles	50 mbps - 100 mbps
5)	Dropped Calls	Yes	Yes	Yes	Improve ments	much better
6)	Voice	Yes	Yes	Yes	Yes	Yes

	Basic Term	1G	2G	2.5G	3G	4G
7)	Video	No	No	No	Yes	Yes
8)	Signals	Analog	Digital	Digital	Digital	Digital
9)	Technologies	AMPS, NMT TACS	GSM	TDMA, CDMA	W-CDMA UMTS	LTE, LTE advanced
10)	Multiple address access system	FDMA	TDMA, CDMA	TDMA CDMA	CDMA	CDMA
11)	Switching type	Circuit switching	Circuit switching for voice & packet switching for data	Circuit switching for voice & packet switching for data	Packet switching except for air interface	Packet switching
12)	Internet service	No internet	Narrow-band	Narrow-band	Broadband	Ultra broadband
13)	bandwidth	Analog	25 MHz	25 MHz	25 MHz	100 MHz
14)	Special chkt	1st wireless camera	digital version of 1G technology	Upgrade version of 2G technology	digital broadband	Very high speeds, All IP

difference betn 4G & 5G

	Specification	4G	5G
1)	Peak data rate	1 Gbps	10 Gbps
2)	Data bandwidth	2 Mbps to 1 Gbps	1 Gbps & higher as per need
3)	Spectral efficiency	30 b/s/Hz	120 b/s/Hz
4)	TTI (Transmission time interval)	1 ms	Varying (100 µs (min) to 4 ms (max))
5)	Latency	10 ms (radio)	<1 ms (radio)
6)	Mobility	350 kmph	500 kmph
7)	Conn^n density	1000/km^2	1000000/km^2
8)	Frequency band	2 to 8 GHz	3 to 300 GHz
9)	Standards	All access convergence including OFDMA, MC-CDMA, NW - LMPS	CDMA & BDMA (beam division multiple access)

1.2 Cellular Systems

- Cellular systems are mobile systems for two-way wireless communication between the fixed part of the system (transmitters or base stations) and the mobile part of the system (mobile stations) which move in the area covered by each base station.
- In a cellular system, the entire coverage area is divided into 'cells' i.e. they implement SDM (Space Division Multiplexing). Each cell is served by a single base station. Each cell has a size depending on the number of users. More the users, smaller the cell size.
- Cell radii ranges from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the country side.
- The shapes of cells are never perfect circles or hexagons actually, it depends on environment, on whether conditions etc. Hexagon shape cellular system is shown in Fig. 1.2.1.

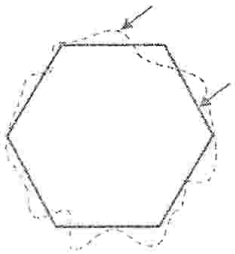


Fig.1.2.1 : Diagrammatic cell

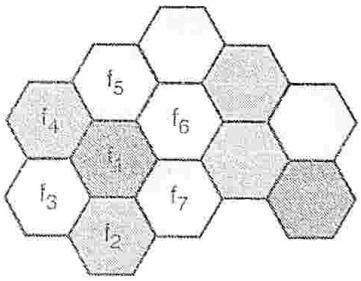


Fig. 1.2.2 : Cellular System with seven cell cluster vs. actual cell coverage

* Electromagnetic spectrum -

→ The electromagnetic spectrum is the complete spectrum (or continuum) of all forms of "light".

→ An electromagnetic waves consist of electric & magnetic fields which vibrate thus making waves.

→ The electromagnetic spectrum consist of radio waves, cell phone waves, microwaves, radar waves, infrared waves, visible light wave, ultraviolet waves, X-ray wave, gamma wave.

→ Properties of electromagnetic waves include speed, frequency & wavelength

speed (s), frequency (f) & wavelength (λ) are related in the formula:

$$s = f \times \lambda$$

→ All light waves travel at a speed of 3×10^8 m/s in a vacuum.

→ All part of the electromagnetic spectrum travel at the same speed

→ Therefore, wavelength & frequency have an indirect relationship.

→ This means that as one part increases, the other decreases.

electromagnetic wave chkt -

1) short wavelength have a high frequency
2) long wavelength have a low frequency.

① Microwaves -

→ Microwaves - have the shortest wavelengths & the highest frequency of radio wave.
• used in microwave ovens.
→ Waves transfer energy to the water in the food causing them to vibrate which in turn transfers energy in the form of heat to the food.
• Used by cell phones & pagers.
• RADAR (Radio Detection & Ranging)
→ Used to find the speed of an object by sending out radio waves & measuring the time it takes them to return.

② Infrared rays -

- Infrared radiation is used in remote controller, commonly for devices such as TVs, DVDs, Home theater systems.
- infrared used in thermal imaging
- The amount of radiation emitted by an object increases with temperature, therefore this techniques allow one to see variations in temperature

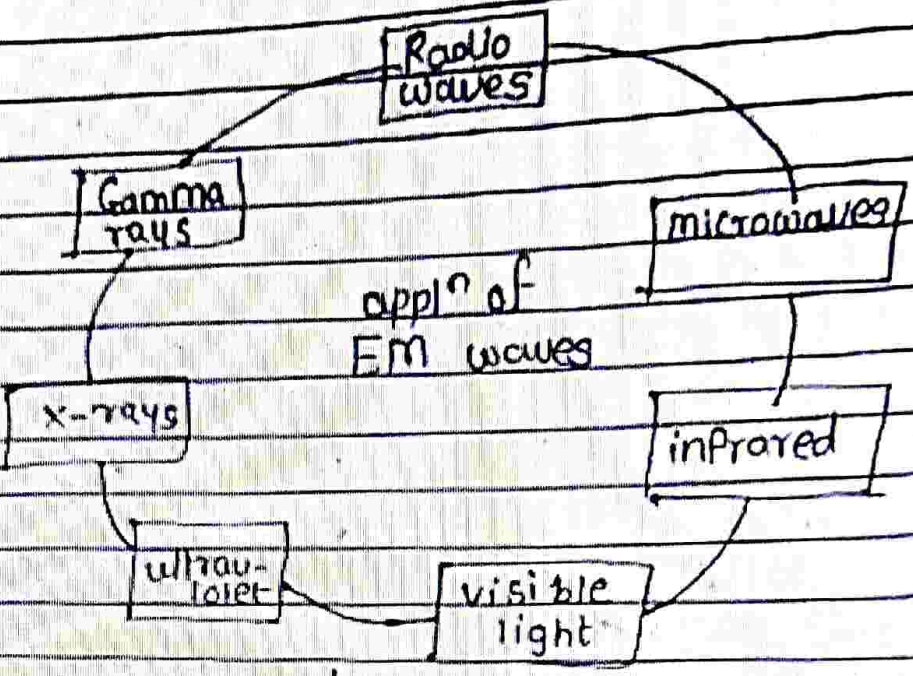


fig: appln of em waves.

(3) Radio waves -

→ radio waves are used for radio comm^n.

→ A radio tuner is necessary to tune in to a particular frequency to receive certain signals.

→ It is also used for broadcasting i.e television transmission

→ The antennae on your television set receive the signal in the form of electro-magnetic curves i.e broadcasted from the television station

→ Radio waves are also used in telecomm^n such as cellular phone.

(2) Visible light -

→ Visible light is also used in other imaging technologies such as mirodome laser.

fiber optics.

⑤ Ultraviolet waves -
→ Higher energy than light waves
→ Can cause skin cancer & blindness in humans
→ Used in tanning beds & sterilizing equipment.

⑥ X-Rays.
- High energy waves
- Used in medicine, industry & astronomy
- Can cause cancer

⑦ Gamma rays
- Highest energy
- Gamma radiation is electromagnetic radiation & high frequency.

Electromagnetic spectrum, electromagnetic radiation can be described as a stream of photons, each traveling in a wave-like pattern carrying energy & moving at the speed of light.

Pillai HOC College of Engineering and Technology

Date:

* Antennas :

→ Wireless comm^n means 'getting rid' of wires and transmitting signal through space without guidance

→ We do not need any medium for the transport of electromagnetic waves.

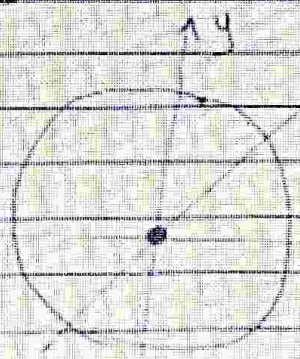
→ Somehow we have to couple energy from transmitter to outside world & in reverse from outside world to receiver. This is done by antennas.

→ Antennas couple electromagnetic energy to & from space to & from wire or co-axial cable.

Types :-

1) Isotropic radiator -

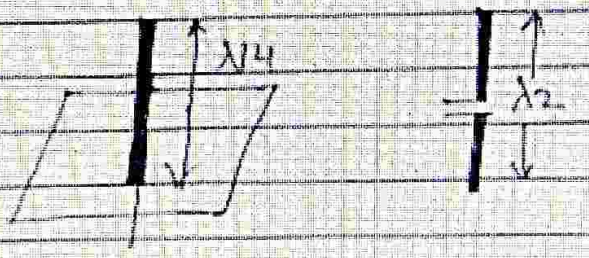
- A point in space radiating equal power in all directions. Iso that point is known as isotropic radiator or antennas.
- The radiation pattern is symmetric in all directions.



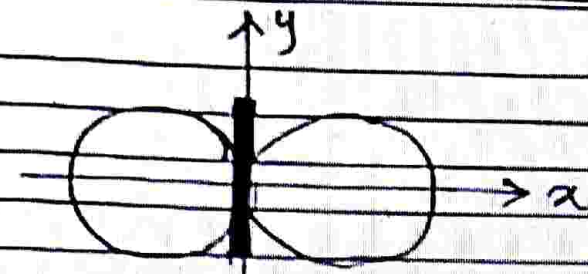
eg: sun

2) Marconi Antenna -
- Real antenna all exhibit directive effect i.e Intensity of radiation is not same in all direction from antenna.
- The simplest real antenna is thin, center fed dipole
- Dipole consist of two colinear conductor of equal length, separated by small feeding gap.
- The length of dipole is not arbitrary for eg. half the wavelength λ of the signal to transmit results in very efficient radiation of energy.

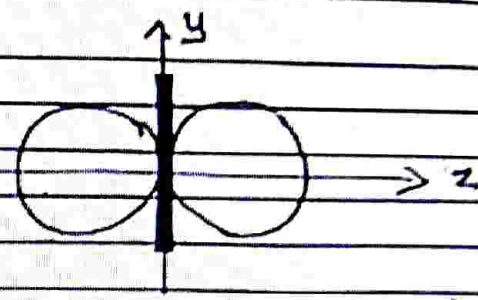
If mounted on roof of car, the length of $\lambda/4$ is efficient



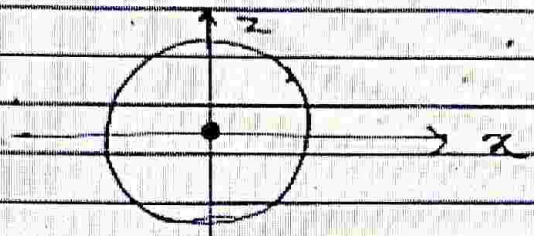
3) Omni-directional antenna - (all direction)
→ A $\lambda/2$ dipole has uniform radiation pattern in one plane & a figure 8 pattern in other two planes.
→ This type of antenna can only overcome
→ Environmental challenges by boosting power level of signal.
→ Challenges could be mountains, valleys, building etc.



side view (xy - plane)



side view (zy - plane)



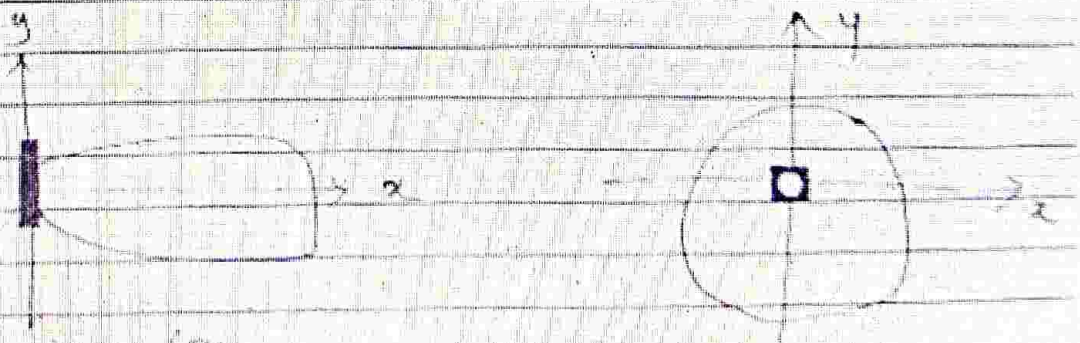
top view (xz - plane)

eg: Router / Mobile
(Home)

a) Directional antenna.

→ It has certain fixed ~~preferented~~ preferential transmission & reception direction.

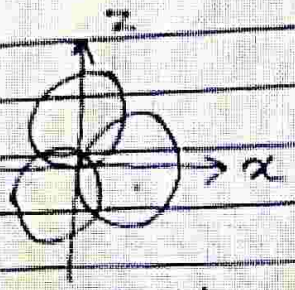
→ It can used between buildings or in valley.



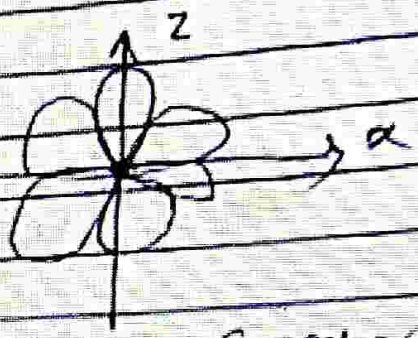
side view (xy - plane)

top view (xy)

5) Sectorized antenna -
- Several directed antennas can be combined on a single pole to construct a sectorized antenna.
- A cell can be sectorized into 3 or 6 sector which enables frequency reuse as directional antenna.



Top view, 3 sector



Top view, 6 sector

eg - Mobile comm^n.

6) multi element antenna array.
- Two or more antennas can also be combined to improve reception by counteracting the negative effects of multi-path propagation. This type of antenna is known as multi element antenna array.
- It allows different diversity schemes like switched diversity or selection diversity.

eg - Satellite tracking system.

7) Smart antenna
- It combines multiple antenna elements with signal processing to optimize antenna reception pattern in response to signal environment.

Signal :-

→ A signal is electrical or electromagnetic current that is used for carrying data from one device or nlw to other.
→ A signal (either) can be analog or digital.
→ It is a key component for comm^n, computing or networking.
→ Signals are physical representation of data. Users of comm^n system can only exchange data through transmission of signals.

Chkt of signal -

1) Signal Amplitude
2) Frequency
3) Wavelength
4) Phase.

1) Signal amplitude -

- Amplitude of data signal is also known as its height or magnitude. It represents strength of transmitted signal.
→ Measurement of signal amplitude is usually carried out in the units of voltage → current.
Analog comm^n - land line phone.
digital comm^n - computer, cellular phone

ii) Frequency -
- It is number of cycles the data signal completes in the form of oscillation in single second
- It represents intensity of transmission & reception in data comm^n n/w.
- It is measured in Hertz (Hz)

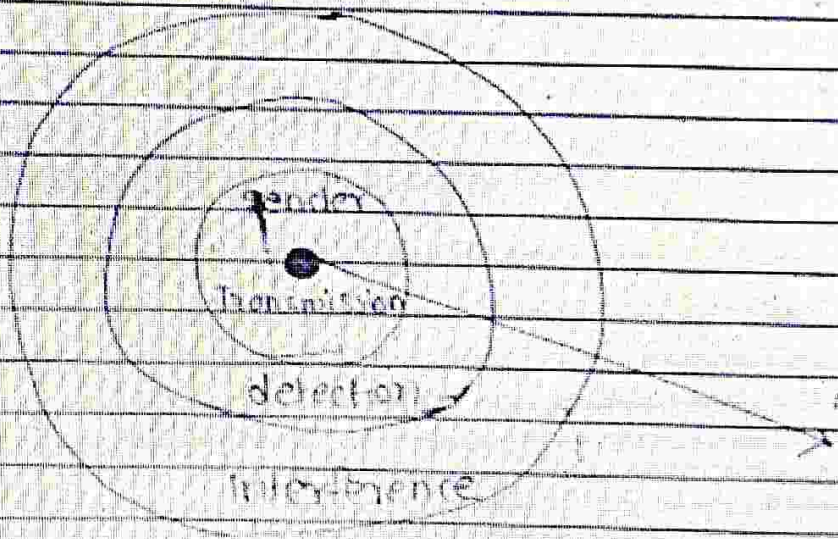
iii) Wavelength -
- It is length of signal which is measured in meters (m)
- It is calculated by finding ratio between speed of light (c) & frequency of signal as c/f.
- It is represented by lambda (λ)

iv) Phase -
- Phase of signal is shift of its amplitude angles which is mesured in degree.
- quality represents change that occur within magnitude of data signal cycle with respect to time.
- When two signals interfere with each other they can cancel each other out if their respective phases are opposite.
- Represented by theta (θ)

Date:

Signal Propagation –

→ Wireless comm^n nw also have sender & receivers of signals.
→ In wireless nw, the signal has no wire to determine the direction of propagation, whereas signals in wired nw only travel along with wire
→ One can precisely determine the behaviour of a signal travelling along this wire. eg. received power depending on the length.
→ For wireless transmission this predictable behaviour is only valid in a vacuum i.e without matter between the sender & the receiver.



Transmission range –
→ Within a certain radius of the sender transmiss is possible i.e. a receiver receives the signal with an error rate low enough to be able to communicate. Beyond that area

e) detection range -
→ Within a second radius of detection of the transmission is possible i.e the transmitted power is large enough to differ from background noise.
→ However, the error rate is too High to establish comm^n.

f) Interference range -
→ within a third even large radius, the sender may interfere with other transmission by adding to the background noise. A receiver will not be able to detect the signals, but the signal may disturb other signals.

Problems arising in signal propagation -

① Path loss of radio signals -
→ In free space radio signals propagate as light does (independently of their frequency) i.e they follow a straight line.
→ If such a straight light exists betn a sender & a receiver it is called line of sight (LOS)
→ Even if no matter exists betn the sender & the receiver (i.e, if there is a vacuum) the signal still experiences the free space loss.

→ Radio waves can exhibit 3 fundamental propagation behaviors depending on their frequency

1) Ground wave - (< 2 MHz)
→ Waves with low frequencies follow the earth surface & can propagate long distance. These waves are used for e.g Submarine comm^n or AM radio.

2) Sky wave — (2 - 30 MHz)
→ Many international broadcasts & amateur radio use these short waves that are reflected at the ionosphere.
→ This way the waves can bounce back & forth between the ionosphere & the earths surface, travelling around the world.

3) Line - of - sight (> 30 MHz)
→ Mobile phone systems, satellite systems, cordless telephones etc use even higher frequencies.
→ The emitted waves follow a straight line of sight.
→ This enables direct comm^n with satellites or microwave link on the ground.
→ However, an additional consideration for ground based comm^n is that the waves are bent by the atmosphere due to refraction.

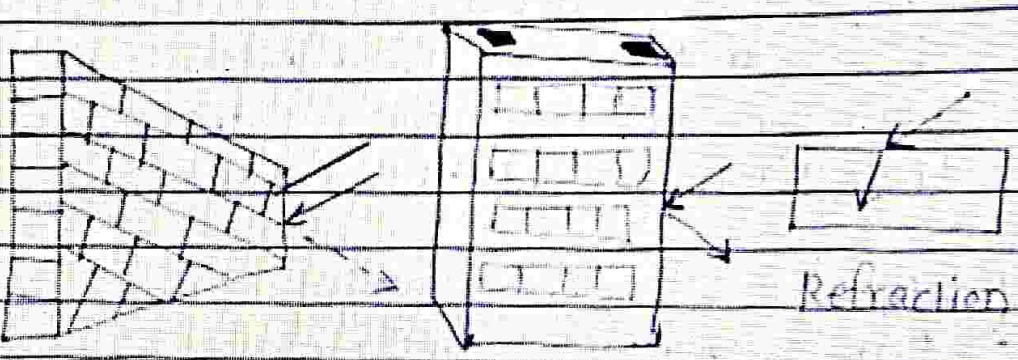
(1) Additional signal propagation effects -
→ Signal propagation in free space almost like a straight line like light but in real life we rarely have a line of sight b/w the sender & receiver of radio signal.

Page No. 35

→ Mobile phones are typically used in bit cities with skyscrapers, on mountains, inside buildings, while driving through an alley etc.

→ An extreme form of attenuation is blocking or shadowing of radio signals due to large obstacles

→ The higher the frequency of a signal the more it behave like light. even small obstacles like a simple wall, a truck on the street, or trees in an alley may block the signal.



Shadowing Reflection

→ Another effect is the reflection of signals

→ If an object is large compared to the wavelength of signal eg. huge buildings, mountains or the surface of the earth, the signal is reflected.

→ The reflected signal is not as strong as the original, as object can absorb some of the signal power

→ Reflection helps transmitting signal as good as no LOS exist

→ This is a standard case of radio transmission signal in cities or mountain areas. Signal transmitted from a sender may bounce off the wall of building several times before they reach the receiver.

→ The more often the signal is reflected, the weaker it becomes.

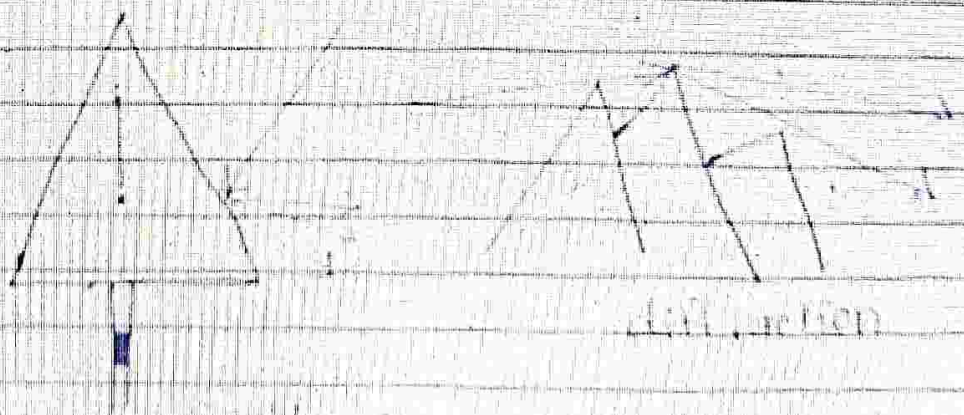
→ This effect occurs bcoz the velocity of the electromagnetic (refraction) waves depends on the density of the medium through which it travels.

→ The waves that travel into a denser medium are bent towards the medium.

→ This is the reason for LOS radio waves being bent towards the earth: the density of the atmosphere is higher closer to the ground.

→ While shadowing & reflection are caused by objects much larger than the wavelength of the signal, the following two effects exhibit the 'wave' character of radio signal. If the size of an obstacle is in the order of the wavelength or less then waves are can be scattered.

→ An incoming signal is scattered into several weaker outgoing signal.



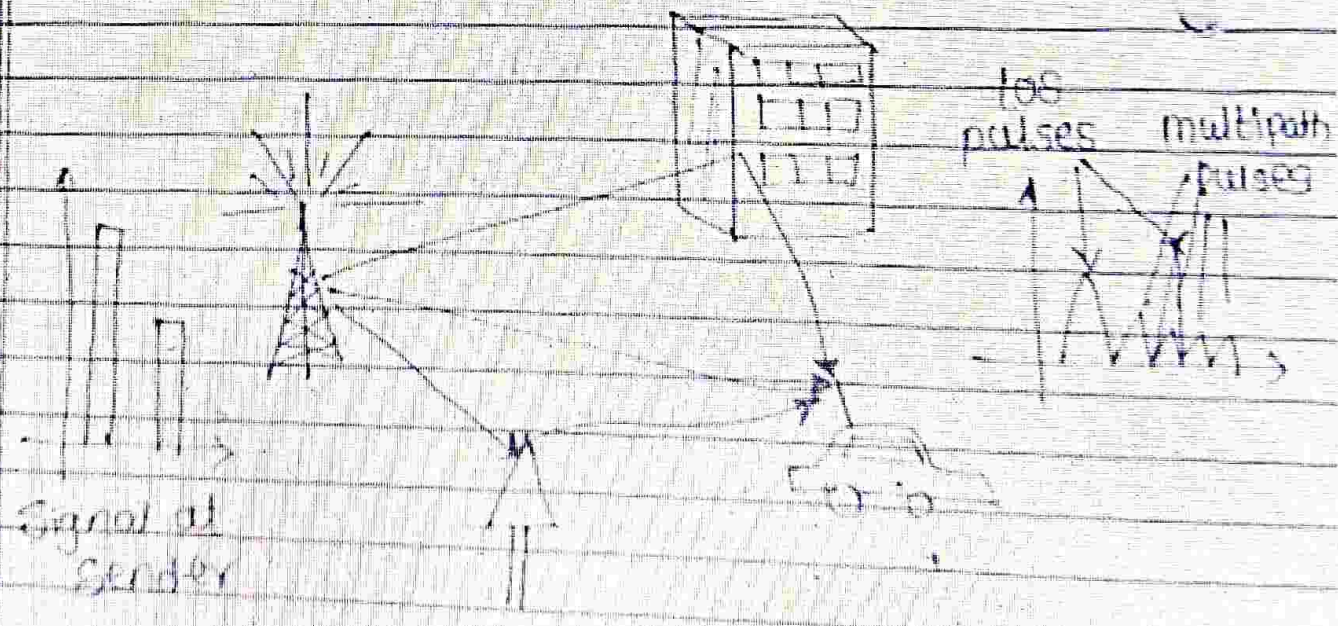
→ Another effect is diffraction of waves. This effect is very similar to scattering. Radio waves will be deflected at an edge & propagate in diff direction.

→ The result of scattering & diffraction are patterns with varying signal strengths depending on the location of the receiver.

(ii) Multi-path propagation:-

→ Together with the direct transmission from a sender to a receiver, the propagation effects mentioned in the previous section lead to one of the most severe radio channel impairments, called multi-path propagation.

→ Radio waves emitted by the sender can either travel along a straight line, or they may be reflected at a large building, or scattered at smaller obstacles.



→ This simplified figure only shows 3 possible path for the signal.

→ In reality, many more paths are possible due to the finite speed of light. Signals travelling along diff paths with diff lengths arrive at the receiver at diff times. This effect is called delay spread.

The original signal is spread due to diff delays of parts of the signal.

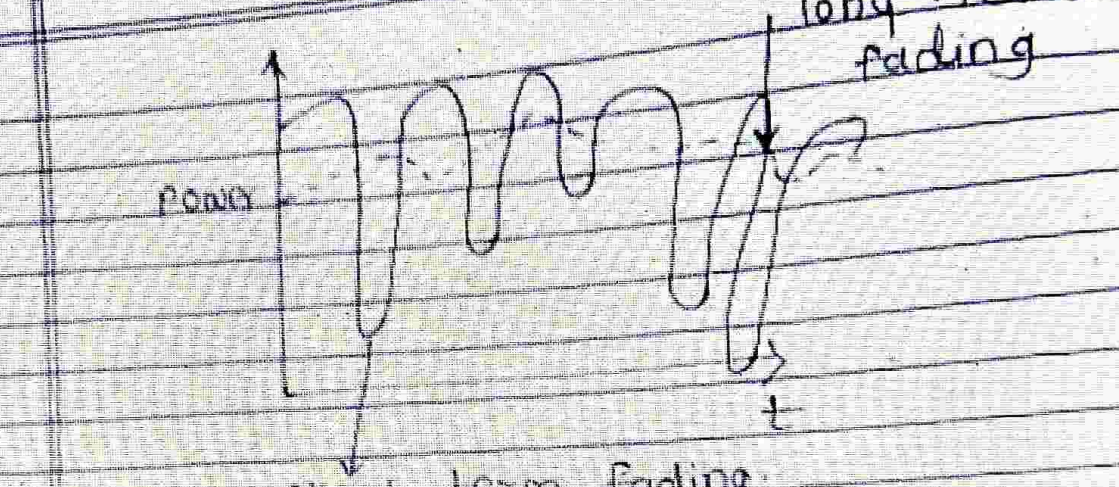
→ This delay spread is a typical effect of radio transmission, bcoz no wire guides the waves along a sig single path as in the case of wired nws.

→ On the sender side both impulses are separated. At the receiver both impulses interfere i.e they overlap in time.

→ Now consider that such each impulses should represent a symbol i.e that one of several symbol could represent a bit.

→ The energy intended for one symbol now spills over to the adjacent symbol, an effect which is called intersymbol interference (ISI)

→ The power of the received signal changes considerably over time. These quick changes in the received power are also called small scale fading.



→ However if these changes are too fast such as driving on a highway through a city, the receiver cannot adapt fast enough & the error rate of transmission increases dramatically if the long-term fading of the received signal.

Date:

multiplexing

analog — fdm, tdm

digital — cdm

* Multiplexing - fdm tdm cdm

→ Multiplexing is not only a fundamental mechanism in comm^n system but also in everyday life.

→ Multiplexing describes how several users can share a medium with minimum or no interference.

→ There are 4 types of multiplexing -

(1) Space division multiplexing - (SDM)

→ For wireless comm^n, multiplexing can be carried out in four dimensions: space, time, frequency & code.

→ In this field, the task of multiplexing is to assign space, time, frequency & code to each comm^n channel with a minimum of interference & a maximum of medium utilization.

→ The term comm^n channel here only refers to an association of sender (s) & receiver (s) who want to exchange data.

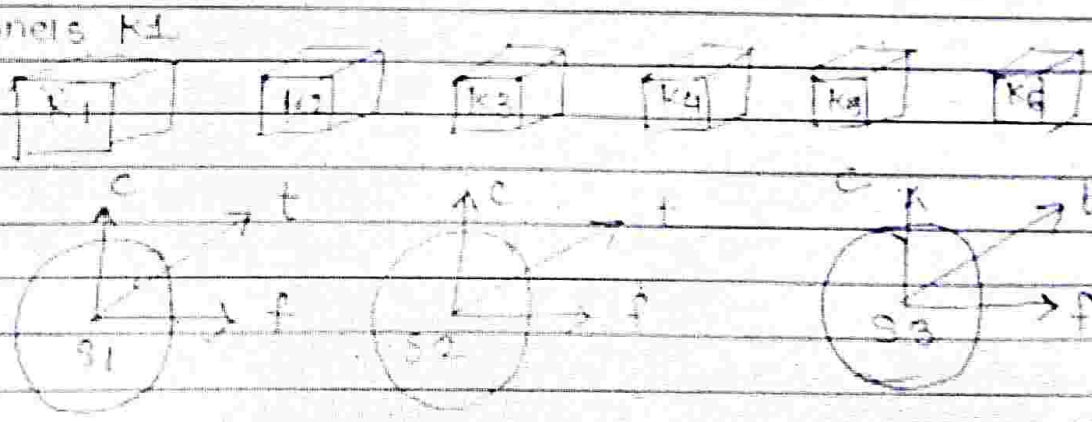


fig: sdm

→ fig shows space division multiplexing.

→ The space is indicated by circles.

There are six channels shown from k1 to k6

→ The channels k1 to k8 are mapped onto the three spaces g1 to g3. This space separates the channels & prevents the interference ranges from overlapping.
→ The space betⁿ the interference ranges is called as guard spaces. Remaining channels k4 to k6 are mapped to remaining 3 spaces.
→ This scheme is used in analog telephone system.

Advantages –
Frequency reuse.

Disadvantages –
→ SDM can't be implemented alone. It has to be implemented along with some other multiplexing scheme.

Applⁿ –
Optical commⁿ, Mobile commⁿ, FM radio.

(2) Frequency division multiplexing (FDM) –

→ FDM describes schemes to subdivide the frequency dimension into several non-overlapping frequency band.
→ Each channel k_i is now allotted its own frequency band as indicated. Senders using a certain frequency band can use this band continuously

Date:

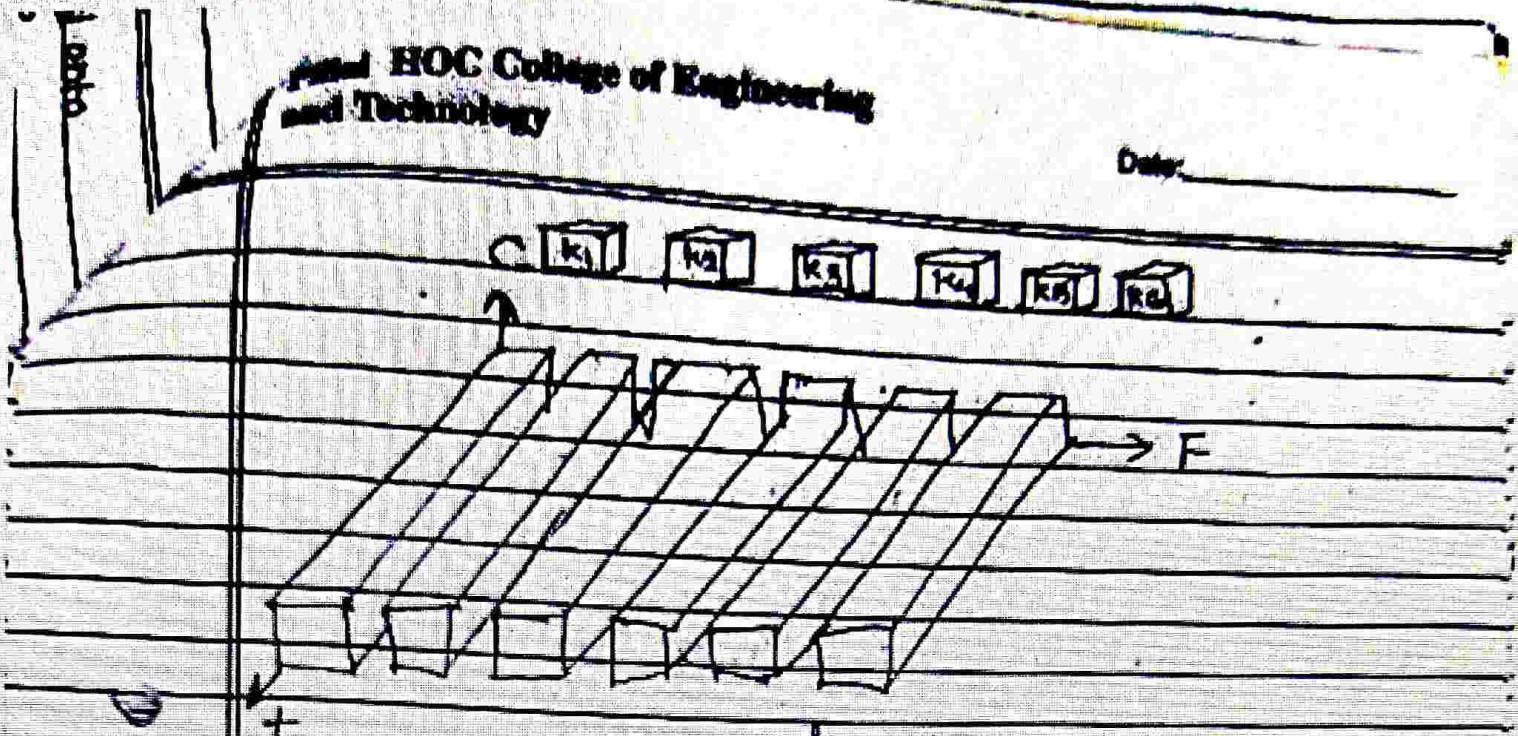


fig - FDM.

→ Again guard spaces are needed to avoid frequency band overlapping. This scheme is used for radio station within the same region; where each radio station has its own freq.

→ This very simple multiplexing scheme does not need complex coordination bet^n sender & receiver. the receiver only has to tune in to the specific sender.

Appln :-

1) Conventional cable television & telephone n/w
2) AM & FM radio broadcasting
3) First generation cellular technology was based on FDM.

Advantages

1) demodulator is easy to design.
2) It helps in increasing the overall system capacity

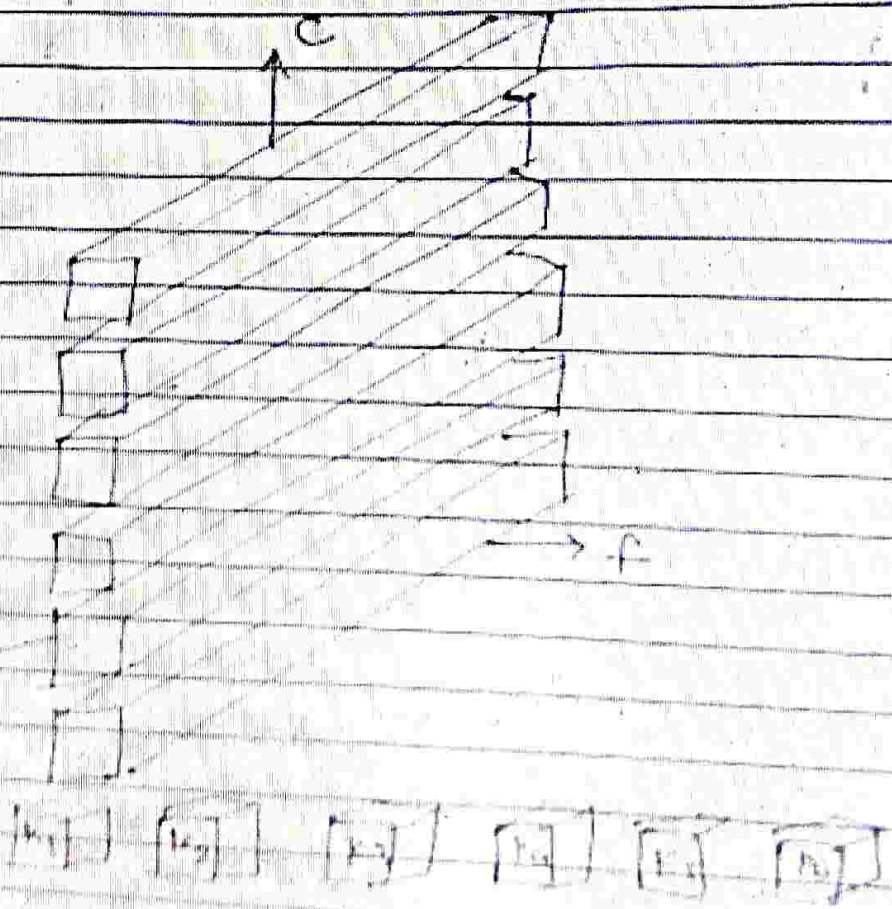
Disadvantages

2) A large no. of modulators, demodulators & filter are required. It increase overall size of the hw.

(3) Code division multiplexing (CDM) -

→ In CDM scheme each user is allocated with the ~~sh~~ typical code. These codes are generated to provide orthogonality & therefore there is no interference betn the code. Each code channel is unique.

→ CDM has built in security. It provides good protection against interference & jamming.



Date:

Advantages –

1) It provides good protection against interference & tripping.
2) More no. of users are accommodated in less frequency spectrum as compared to TDM & FDM schemes.

disadvantages –

1) Overall system & specifically receiver is complicated.
2) As the no. of users increases, the quality of signal reduces.

Appln –

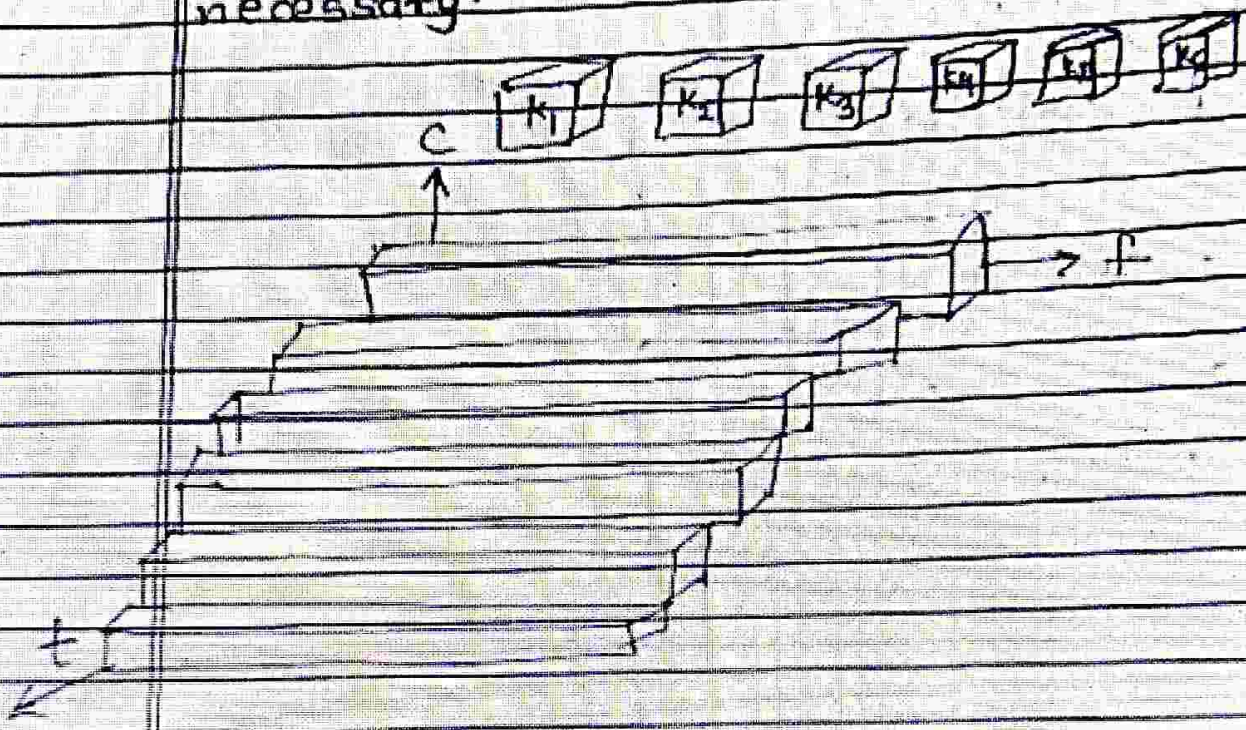
1) Military comm^n.
2) Mobile comm^n.

(a) Time division multiplexing – (TDM)

1) A more flexible multiplexing scheme for typical mobile comm^n is time division multiplexing (TDM).
2) Here a channel is given the whole bandwidth for a certain amount of time i.e. all senders use the same frequency but at different points in time.
3) Again guard spaces, which now represent time gaps, have to separate the diff periods when the senders use the medium.

→ If two transmissions overlap in time, this is called co-channel interference.

→ To avoid this type of interference, between precise synchronization betn different senders is necessary.



→ Frequency & time division multiplexing can be combined i.e a channel ki can use a certain frequency band for a certain amount of time.

→ The mobile phone standard GSM uses this combination of frequency & time division multiplexing for transmission betn a mobile phone & so called base station.

Advantages -

1) TDM systems are more flexible than FDM.

2) full available channel bandwidth can be utilized for each channel.
3) TDM circuitry is not complex.

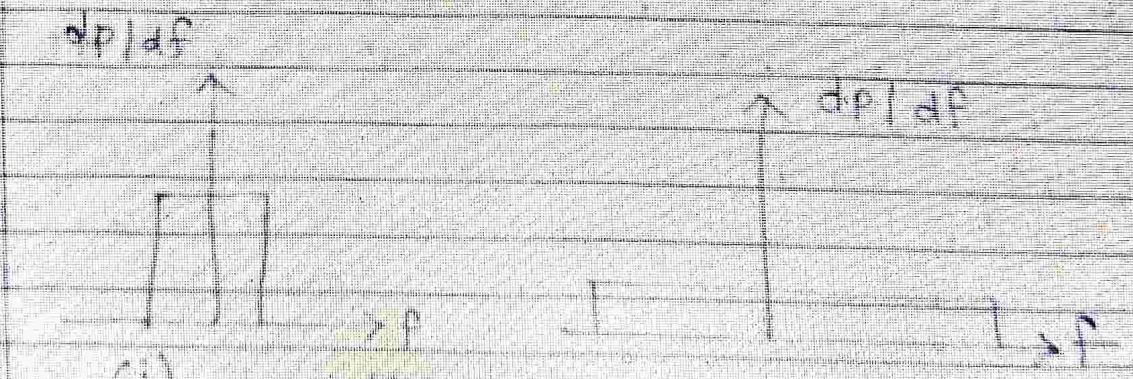
Disadvantages -
1) Synchronization is required in TDM
2) Complex to implement.

Appln -
1) It is used for some telephone system.
2) It is used in wire-line telephone lines.
3) It is widely used in telephone & cellular ntw.

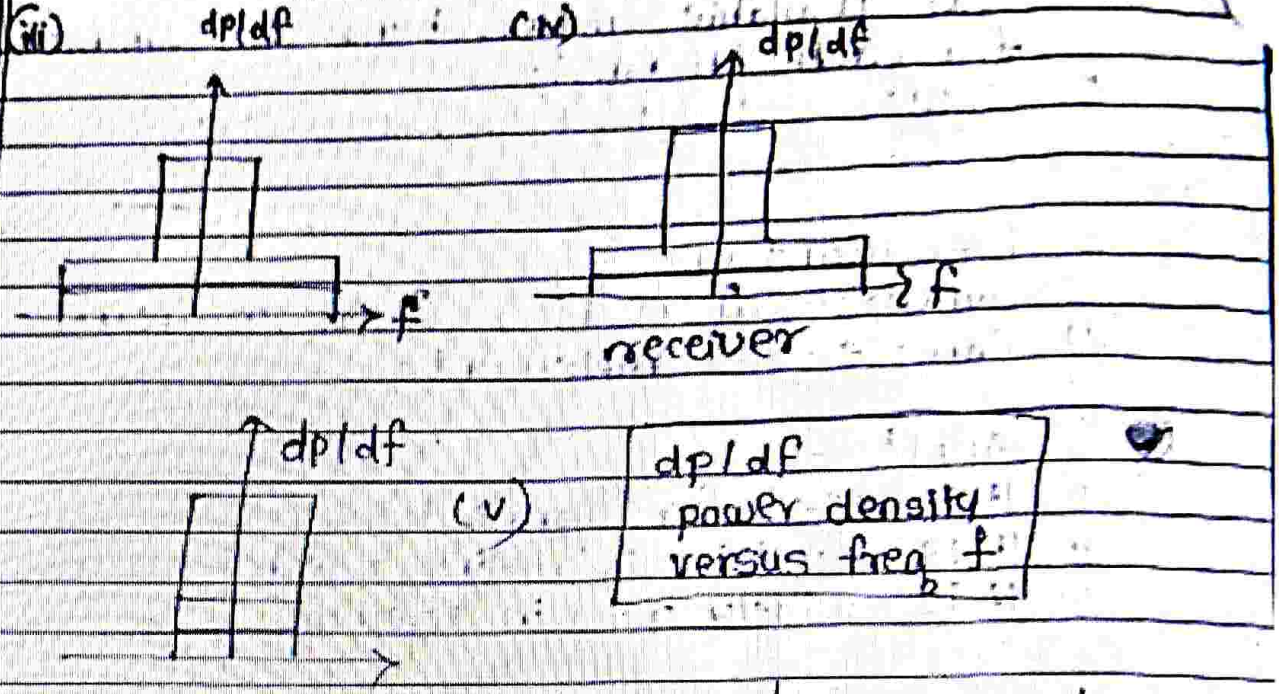
* Spread Spectrum -

→ Spread spectrum techniques involve spreading the bandwidth needed to transmit data - which does not make sense at first sight.

→ Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference.



(1) sender



→ diagram (i) shows an idealized narrowband signal from a sender of user data

→ The sender now spread the signal in step(ii) i.e converts the narrowband signal into a broadband signal. The energy needed to transmit the signal is the same, but it is now spread over a large frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data.

→ During transmission, narrowband & broad-band interference add to the signal in step(iii) The sum of interference & the user signal is received

→ The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while

spreading the narrowband interference & leaving the broadband interference.

→ In step (v) the receiver applies a bandpass filter to cut off frequencies left & right of the narrowband signal.

→ finally the receiver can reconstruct the original data bcoz the power level of the user signal is high enough i.e the signal is much stronger than the remaining interference.

Spreading the spectrum can be achieved in 2 different way

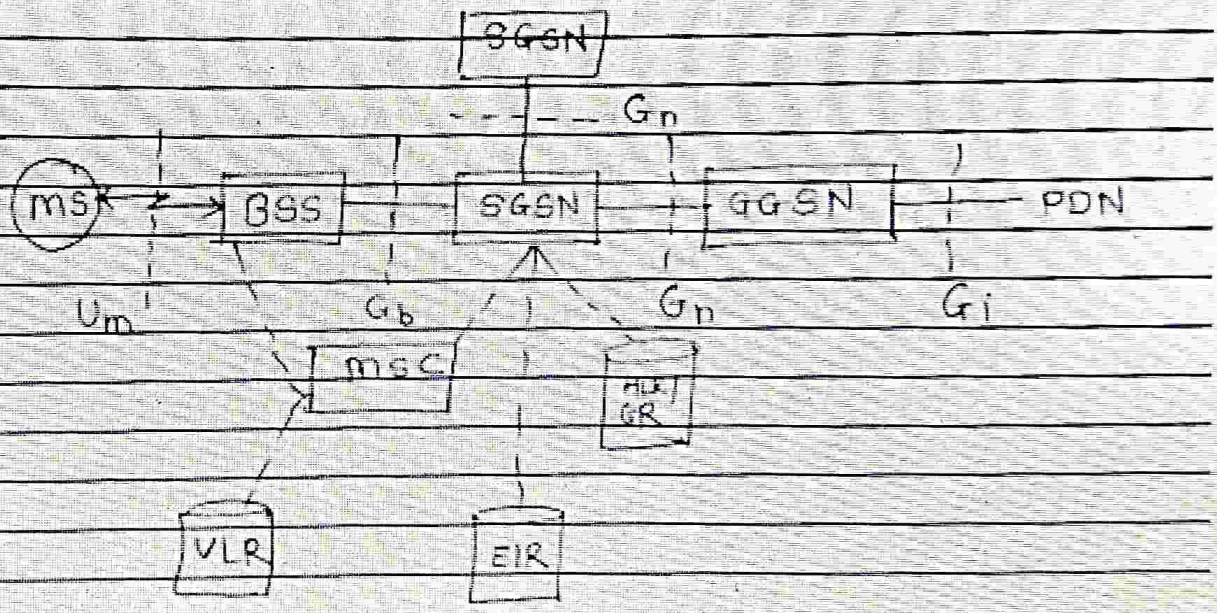
i) Direct sequence spread spectrum

ii) Frequency hopping spread spectrum

* GPRS system

→ The general packet radio service (GPRS) provides packet mode transfer for appl^n that exhibit traffic patterns such as frequent transmission of small volumes or infrequent transmission of small or medium volumes according to the requirement specification.

GPRS architecture



→ The GPRS architecture introduces two new network element, which are called GPRS support nodes (GSN) & are in fact routers.

→ All GSNs are the integrated into the standard GSM architecture & many new interfaces have been defined.

→ The gateway GPRS support node (GGSN) is the inter-working unit betn the GPRS n/w & external packet data n/w (PDN).

→ This node contain routing information for GPRS users, performs address conversion, & tunnels data to a user via encapsulation.

→ The GGSN is connected to external n/ws via the Gi interface & transfer packet to the SGSN via an IP-based GPRS backbone n/w (Gn interface).

→ The other new element is the serving GPRS support node (SGSN) which supports the MS via the Gb interface.

→ The SGSN, for eg requests user address from the GPRS register (GR), keeps track of the individual MS's location & is responsible for collecting billing information & perform several security fun^n such as access control.

→ The SGSN is connected to a BSC via frame relay & is basically on the same hierarchy level as an MSC.

→ The GR, which is typically a part of the HLR, stores all GPRS relevant data.

GGSNs & SGSN can be compared with home & foreign agents respectively in a mobile IP n/w.

difference betn GSM & GPRS.

	GSM	GPRS
1)	GSM is standard bearer of 2G technology	GPRS is be upgrade over the basic GSM features. It allow the mobile handset to obtain much higher data speed than what standard GSM can offers.
2)	In GSM traffic & signaling follow different multi-frame structure i.e 51 frame MF used for signaling & 26 frame MF used for traffic	In GPRS traffic & signaling both follow common multi-frame structure i.e 52 frame MF used for both signaling as well as traffic
3)	GSM used circuit switching traffic.	GPRS used for packet switching traffic
4)	In GSM time slot is allocated both in uplink & downlink due to these radio resource allocation in GSM is called as symmetric	In GPRS radio resources allocation is asymmetric i.e for eg. it is possible to allocate the time slot only in downlink not in uplink when user is only downlink downloading the file
5)	In GSM location area concept is used	In GPRS routing area concept is used.

* Gsm mobile services -

→ Gsm permits the integration of different voice & data services & the interworking with existing networks.

→ Services make a nw interesting for customers. Gsm has defined 3 different categories of services - bearer, tele, and supplementary services.

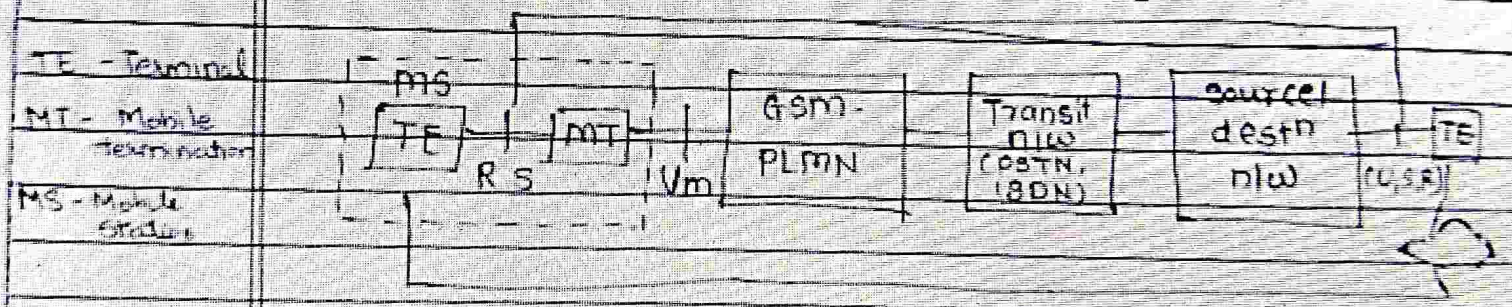


fig: Bearer & tele services reference model

→ A mobile station MS is connected to the Gsm public land mobile nw (PLMN) via the Um interface. (Gsm - PLMN is the infrastructure needed for the GSM nw)

* GSM system architecture –

→ As with all systems in the telecomm^{n} area, GSM comes with a hierarchical, complex system archi- comprising many entities, interfaces & acronyms.

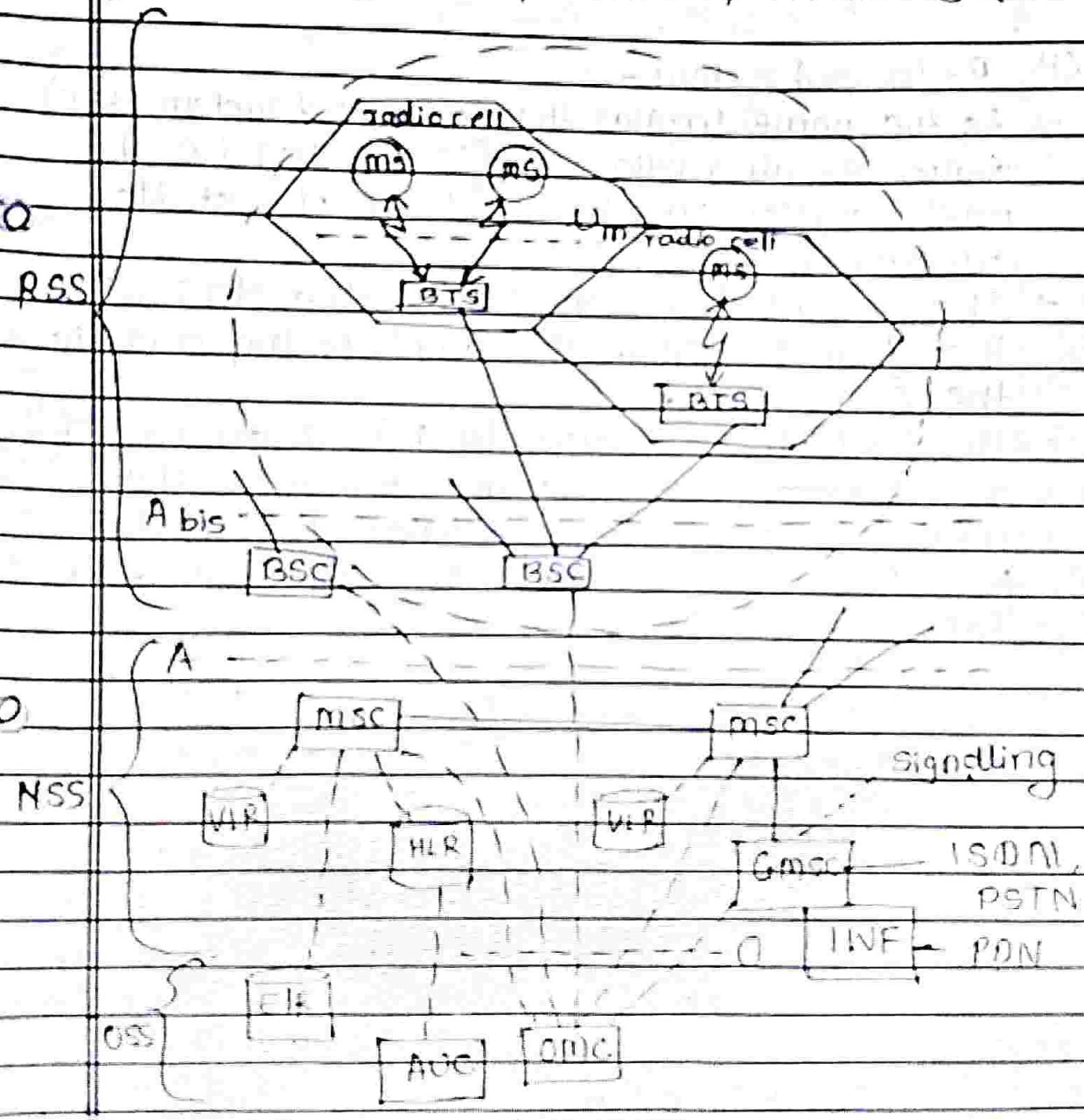


fig. GSM archi

2.1.8 GSM Security

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

Q. Explain in short different algorithm used for authentication and privacy in GSM? **(May 12, Dec. 19, 10 Marks)**

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

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

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

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

1. Access control and authentication

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

2. Confidentiality

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

3. Anonymity

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

Authentication

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

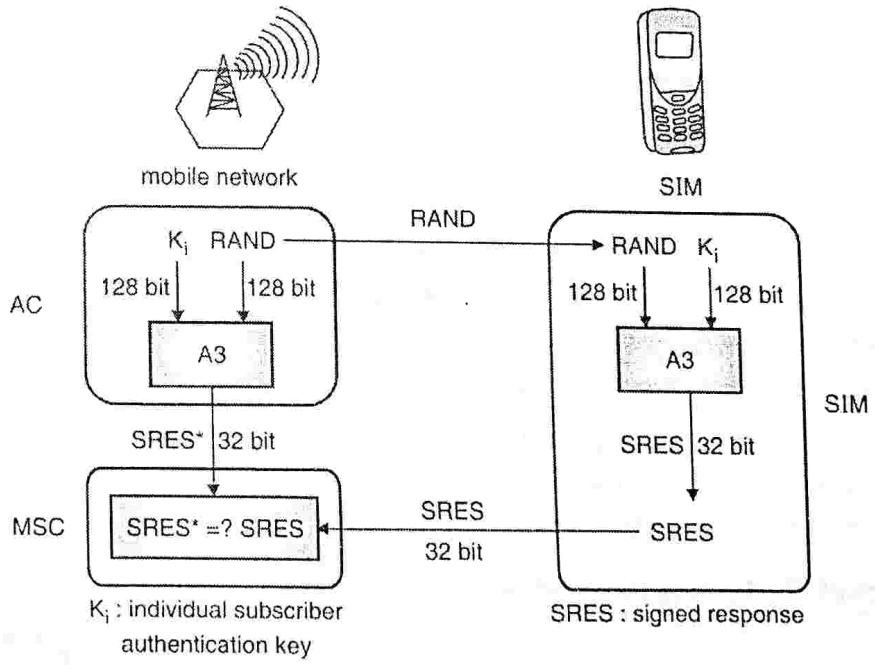


Fig. 2.1.12 : Authentication in GSM

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

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

Encryption

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

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

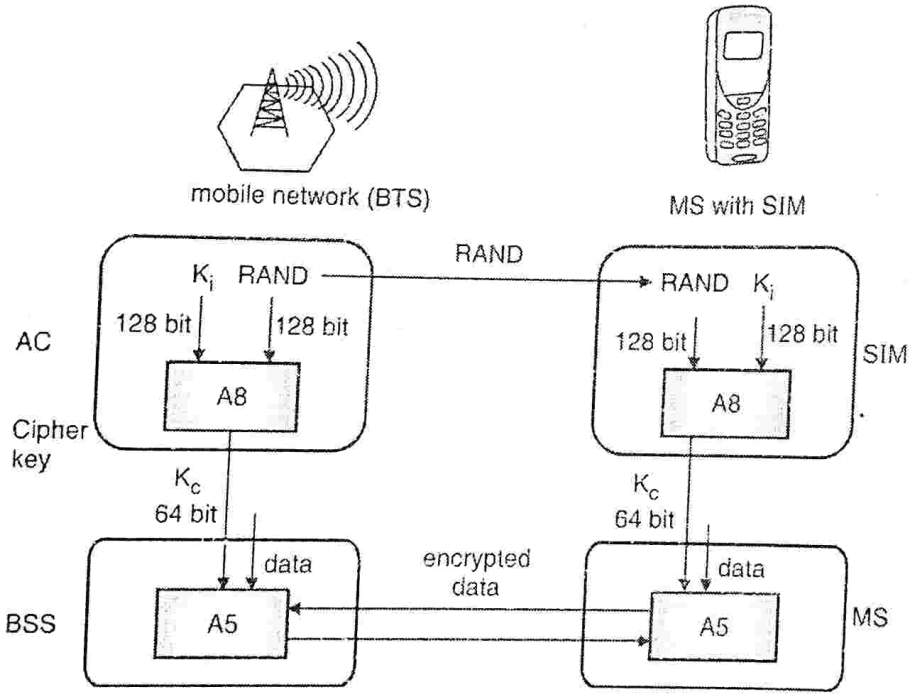


Fig. 2.1.13 : Data encryption in GSM

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

2.1.7 Handover in GSM

MU - May 15, May 16

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

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

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

There are two basic reasons for handover :

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

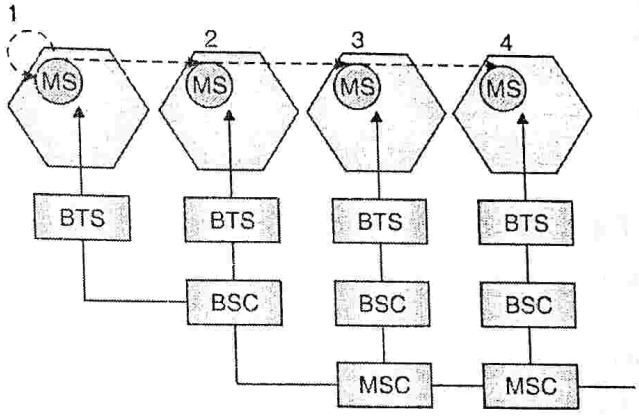


Fig. 2.1.10 : Handover scenario in GSM

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

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

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

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

1. UTRAN

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

Module 2 bekar jam bekar lesson

Jast load ny ghyaycha

Lihu vatal tar liha nytar zopun ya