Question Bank

Assignment 1

1. Define the following terms :

Channel: Wireless channel can be defined as the medium between two end points of a communication system. One end point can be a transmitter (denoted by Tx) that transmits or sends the signal that will propagate through the wireless medium . The transmitted signal will be received by the other end point or the receiver (denoted by Rx). There is no wired or physical connection between the two endpoints in a wireless channel. The signal is propagated through radio frequency

Multipath propagation : When a signal is propagated from a sender, it will be transmitted in many directions. The signals will then travel in separate ways, bounce on objects, and spread. The signals that reach the same receiver can have taken different routes but still ended up at the same end destination. This is called multipath. The problem with this is that if two signals are sent simultaneously from the sender and take different routes and end up at the same receiver, they will probably reach the destination at different times. This can make it hard to interpret the signal sent from the beginning.

Fading : In wireless communication, fading is a phenomenon in which the strength and quality of a radio signal fluctuate over time and distance. Fading is caused by a variety of factors, including multipath propagation, atmospheric conditions, and the movement of objects in the transmission path. Fading can have a significant impact on the performance of wireless communication systems, particularly those that operate in high-frequency bands.

Simplex channel, Duplex channel, FDD, TDD, Multiple Access, Processing gain in Spread spectrum system, subcarrier and subchannel.

Simplex channel: A simplex channel is a communication channel that allows data transmission in only one direction. It means that data can flow in one direction only, typically from a transmitter to a receiver. Examples include radio and television broadcasts.

Duplex channel: A duplex channel is a communication channel that allows data transmission in both directions simultaneously. This enables two-way communication,

where data can be sent and received simultaneously. Examples include telephone conversations and most internet connections.

FDD (Frequency Division Duplex): FDD is a method used in communication systems where the transmission and reception of data occur on separate frequency bands simultaneously. This allows for simultaneous two-way communication, with one frequency band used for transmitting and another for receiving.

TDD (Time Division Duplex): TDD is a method used in communication systems where transmission and reception of data occur alternately in time over the same frequency band. It means that the same frequency is used for both transmitting and receiving, but they take turns in time.

Multiple Access: Multiple access refers to the ability of multiple users or communication devices to share the same communication channel simultaneously. It allows multiple users to transmit and receive data over the same channel without significant interference.

Processing gain in Spread Spectrum systems: Processing gain refers to the ratio of the spread bandwidth to the original information bandwidth in a spread spectrum system. Spread spectrum techniques spread the signal energy over a wider bandwidth, increasing resistance to interference and providing security. Processing gain is a measure of how effectively this spreading is achieved.

Subcarrier and Subchannel:

Subcarrier: In communication systems, a subcarrier is a frequency within the main carrier frequency that carries additional information. Subcarriers are used for various purposes like carrying audio, video, or data signals in multiplexing systems.
Subchannel: A subchannel refers to a portion of the total available bandwidth within a communication channel that is allocated for specific data transmission. Subchannels can be used to separate different streams of data within the same channel, allowing for multiple simultaneous transmissions.

2. Compare FDMA & TDMA on following points: Definition, Sharing Resource, Guard band requirement, Synchronization requirement, Filtering, ISI, Capacity, and Channel BW.

Features	FDMA	TDMA

Definition	Divides the available frequency bandwidth into multiple non-overlapping sub-channels, each assigned to a different user.	Divides the available time slot into multiple frames, each further divided into time slots assigned to different users.
Sharing Resource	Frequency	Time
Guard Band Requirement	Yes, required between adjacent channels to prevent interference.	Yes, required between adjacent time slots to avoid overlapping transmissions.
Synchronization Requirement	Not required.	Required for accurate timing of slot boundaries to avoid collisions.
Filtering	Filters are used to separate signals in different frequency bands.	Not typically used for filtering, as users transmit in different time slots.
ISI (Inter-Symbol Interference)	Less susceptible to ISI as channels are separated in frequency.	More susceptible to ISI if users share the same channel within a frame due to overlapping symbols.
Capacity	Limited by the available bandwidth and the number of sub-channels that can be created.	Can support more users than FDMA due to efficient time division and potential for reuse within a cell.
Channel BW	Each user has a dedicated portion of the total bandwidth.	Users share the entire bandwidth but only transmit during their allocated time slots.
Stability	It requires stability of high carrier efficiency.	It does not require stability of high carrier efficiency.
Power	Power efficiency is less.	Power efficiency is high.
Used in	It is basically used in GSM and PDC.	It is basically used in advanced mobile phone systems.

3. Explain CDMA has infinite theoretical capacity but is limited by the number of users.

CDMA is interference limited because the introduction of each additional user raises the overall level of interference at the base station receivers. Each mobile radio introduces interference as a function of power level, synchronization and code cross-correlation with other CDMA signals. The number of CDMA channels allowed depends
on the level of total interference that can be tolerated. Figure 5.6 illustrates the basic difference between interference-limited systems, such as CDMA, and dimension-limited systems, such as TDMA

4. List the main characteristics of CDMA.

1. **SOFT CAPACITY**: CDMA systems are able to accept users over its hard capacity limit. When a mobile user requests access to a system that has reached hard capacity, the cell may allow this user onto its network because it has a uniquely coded signal. To accommodate this new user, the quality of service of the cell is decreased to an allowable level. This alleviates the occurrence of dropped calls due to cells operating at hard capacity.

2. **SOFT HANDOFFS**: TDMA and FDMA suffer from hard handoffs. Since each user is designated a certain transmission slot within a cell, it must be reassigned to a new slot as it moves to another cell. If the new cell has reached capacity, then the call is dropped. CDMA eliminates the hard handoff through a technique logically labeled the soft handoff. Once a mobile user approaches the fringe of a cell, it may transmit to adjacent cells simultaneously because it has a uniquely encoded signal. Once it moves closer to one base station and farther from the others, the user transitions smoothly to just one base station. Because of the innovative soft capacity of CDMA cells, even if the adjacent cell is at hard capacity, it will still accept the new user.

3. **POWER CONTROL**: Rather than blindly broadcasting signals at full power, CDMA systems utilize power control to decrease system noise and interference, thus enhancing network quality. Mobile users are required to transmit at a minimum power level necessary for the signal to reach the base station. This eliminates interference into adjacent cells and decreases the amount of noise on the system.

4. **INCREASED USER CAPACITY:** CDMA has a higher user capacity than that of TDMA or FDMA. The full utilization of system resources (frequency bandwidth and time) allows more users access to the system. In addition, the code word length used to encode the signals most stringently limits user capacity. Thus, as

long as adequate power is available to the mobile user, a system may have as many users as its code length can support.

5. **SECURITY**: CDMA inherently secures its signals by encoding the user transmission in a unique code. Eavesdropping listeners must have knowledge of that code in order to decipher the signal.
6. **BANDWIDTH ON DEMAND:** Since CDMA systems utilize the entire available frequency spectrum, each user that requires additional resources with which to transmit may get it without disrupting the quality of service for other users.

Ye GFG ka:-

1. It allows more users to connect at a given time and thus provides improved data and voice communication capacity.
2. A full spectrum is used by all the channels in CDMA.
3. CDMA systems make the use of power control to eliminate the interference and noise and to thus improve the network quality.
4. CDMA encodes the user transmissions into distinct and unique codes in order to secure its signals.
5. In CDMA systems all the cells can thus use the same frequency.
6. CDMA systems have a soft capacity.Thus there is no particular limit to the number of users in a CDMA system but with increase in the number of users the performance degrades.

5. What are the main features of Spread Spectrum?

Characteristics of the Spread Spectrum are:

1. Higher channel capacity.
2. Ability to resist multipath propagation.
3. They cannot easily be intercepted by any unauthorized person.
4. They are resistant to jamming.
5. The spread spectrum provides immunity to distortion due to multipath propagation.
6. The spread spectrum offers multiple access capabilities.

6. Draw the block diagram of DSSS and FHSS transmitter and receiver.

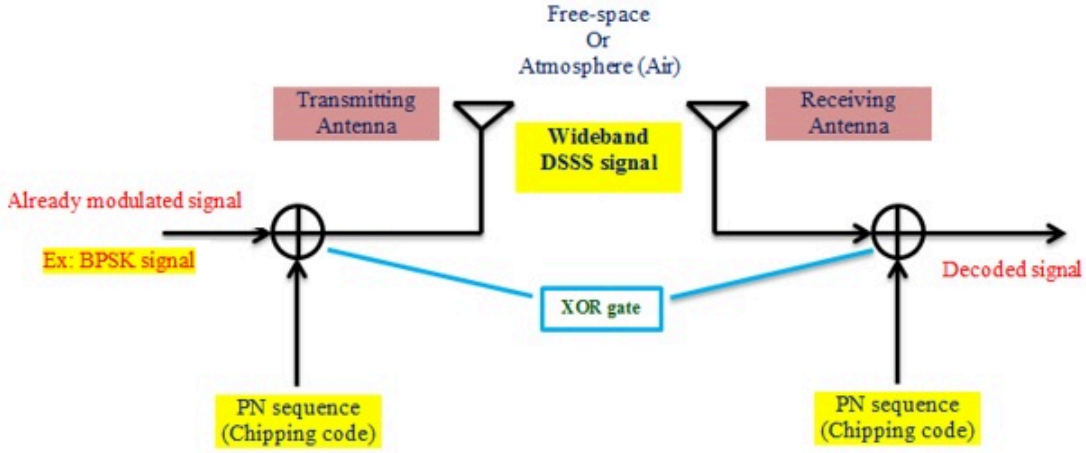
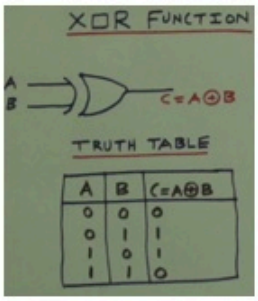
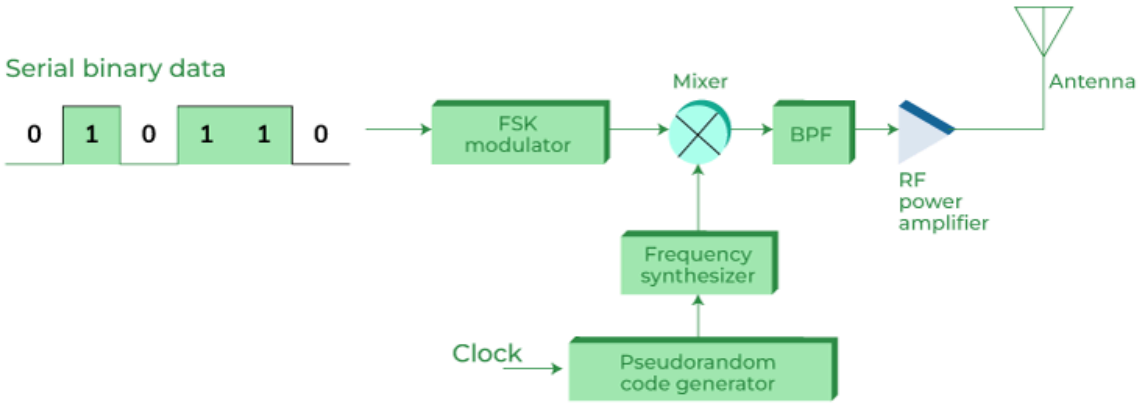


Fig: DSSS Communication System

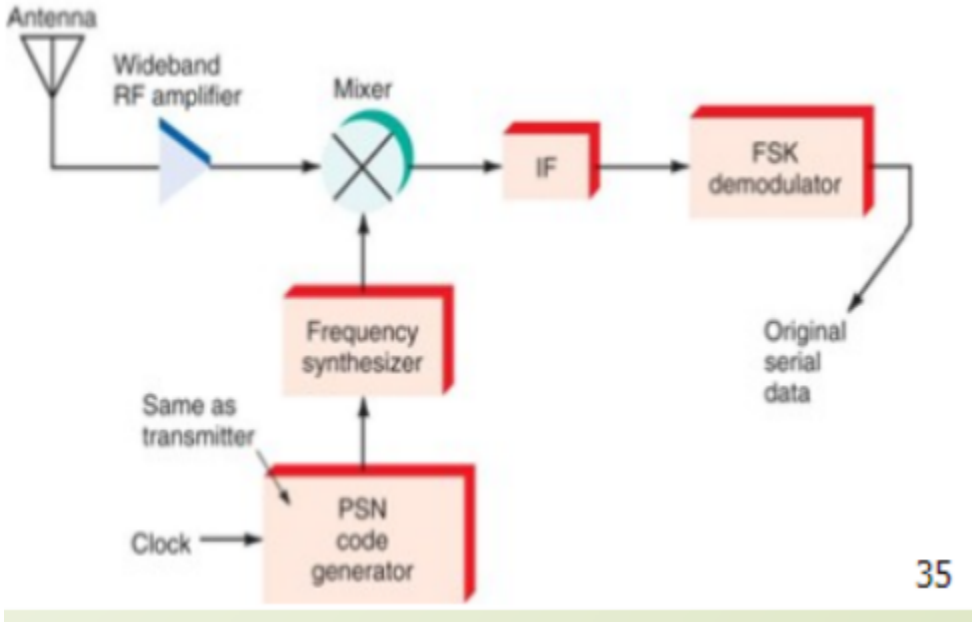
- DSSS is the most widely used technology for SS
- PN (Pseudo-noise) sequence is used to modulate already modulated signal. Pseudo means semi-random.
- Transmitted signal BW >> information signal BW
- XOR technique is used to combine input data stream with PN sequence (spreading code)
- PN codes produced by the transmitter are already known by the receiver.
- At the receiver dispreading is done. The receiver can use the same PN sequence to reconstruct the information signal.
- Received signal is correlated with the PN sequence to recover data and reject interference.



FHSS Transmitter



FHSS Receiver



Characteristics	FHSS	DSSS
Signal Transmission Speed	FHSS signal transmission speed is slow.	DSSS signal transmission speed is high.
Size of Network	The size of the FHSS network is small to medium.	Size of DSSS network is large
Price	Less Expensive	More Expensive
Complexity	Complexity is less	Complexity is More
Reliable	Less reliable	More reliable
Communications	FHSS is suitable for single- point and multipoint communications.	DSSS is suitable for point- to-point communications.
Rate of Signal Transmission	The FHSS signal transmission rate is 3 Mbps.	The DSSS signal transmission rate is 11 Mbps.
Abrreviation	Frequency-hopping spread spectrum	Direct-Sequence Spread Spectrum
Examples	It is used in military and industrial applications.	It is used in consumer applications such as wireless LANs, GPS, and Bluetooth.

7. List the properties of PN code.

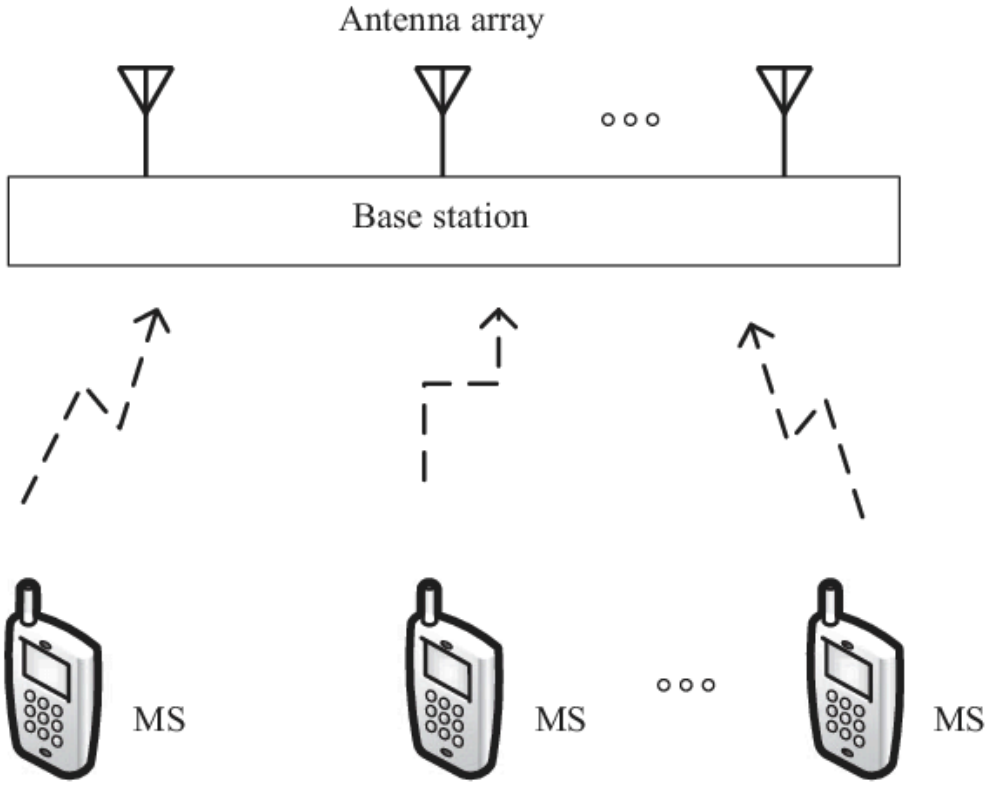
1. Balance property: The number of binary output zeros and the number of binary output ones in a single period differs by at most one.
2. Run length property: A sequence of consecutive 'l's, or 'O's, is called a 'run' and the number of '1's and '0's is the run length.
3. 0's differ only by one: The number of '1's is just one more than the number of '0's.
4. Maximum length sequence: When the period value is equal to 2 to the power M minus 1, the PN sequence is called the maximum length sequence or M sequence.

8. Explain SDMA in brief with suitable illustrations.

Space-division multiple access (SDMA) is a wireless communication technique that increases capacity by dividing physical space into independent channels. It utilizes multiple antennas at the transmitter and receiver to create parallel communication paths.

SDMA is based on the concept of spatial reuse, which allows multiple users to share the same frequency band as long as they are separated by a sufficient distance. This is achieved by using multiple antennas at the transmitter and receiver to create focused

signal beams. Each beam can be used to communicate with a different user, without interfering with the other users.
SDMA is a key technology in 4G and 5G cellular networks. It is also used in other wireless communication systems, such as Wi-Fi and satellite communications.



9. List the data rate, frequency band, services offered and technology used in 1G to 5 G mobile systems.

Technology	1G	2G/2.5G	3G	4G	5G
Bandwidth	2kbps	14-64kbps	2mbps	200mbps	>1gbps
Technology	Analog cellular	Digital cellular	Broadbandwidth/ CDMA/IP Technology	Unified IP and seamless combo of LAN/WAN/WLAN	4G+WWWW
Service	Mobile telephony	Digital voice, Short messaging	Integrated high quality audio, video and data	Dynamic information access, variable devices	Dynamic information access, variable devices with AI capabilities
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit/ circuit for access network and air interface	Packet except for air interface	All packet	All packet
Core Network	PSTN	PSTN	Packet network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal & Vertical	Horizontal & Vertical

10. If 20 MHz of total spectrum is allocated for a duplex wireless cellular system and each simplex channel has 25 KHz RF bandwidth, find: The number of duplex channels

Total bandwidth = $20MHz$

Channel Bandwidth = $25\ KHZ * 2\ simplex\ channels$

= $50\ KHz$

Therefore

Total number of duplex channels= $\frac{20{,}000}{50}$

= $400Channels$

Parameters	FDMA	TDMA	CDMA
Full Form	The term FDMA is an acronym for Frequency Division Multiple Access.	The term TDMA is an acronym for Time Division Multiple Access.	The term CDMA is an acronym for Code Division Multiple Access.
Mode of Operation	FDMA shares one single bandwidth among various stations by splitting it into sub-channels.	TDMA only shares the time of transmission via the satellite and not the channel.	The CDMA shares both- time and bandwidth among various stations by assigning a different code for every slot.
Idea of Transmission	It segments a single band of frequency into various disjoint sub-bands.	It segments the sending time of data into disjoint time slots- in a fixed or demand-driven pattern.	It spreads one spectrum into multiple slots by making use of orthogonal codes.
Code word	The FDMA doesn't need a codeword.	The TDMA also needs no codeword.	The codeword is a prerequisite in the case of the CDMA.
Synchronization	FDMA does not require any synchronization.	TDMA requires synchronization.	CDMA also requires no synchronization.
Data Transmission Mode	Transmission occurs via a continuous signal in FDMA.	Transmission occurs via signals in bursts.	Transmission occurs via digital signals.
Rate of Data	FDMA supports a low rate of data.	TDMA supports a medium rate of data.	CDMA supports a high rate of data.
Flexibility	FDMA is a little flexible.	Flexibility is moderate in TDMA.	CDMA is highly flexible in nature.
Terminals	Every terminal possesses its own uninterrupted frequency.	Every terminal on the same frequency stays active for a very short time.	Every terminal can stay active during the same moment and the same place without any interruption.
Separation of Signals	It occurs by the process of filtration in the frequency domain.	It occurs by synchronizing the time domain.	It occurs via codes along with some special receivers.
Scheme of Transmission	It is continuous for FDMA.	It is discontinuous for TDMA.	It is continuous for CDMA.
Capacity of Cells	FDMA has a very limited cell capacity.	TDMA also has a very limited cell capacity.	CDMA does not possess any limit on a channel's capacity- but this system is interference-limited.

Assignment 2

1. Define the following terms:

Frequency reuse: Technique for using a specified range of frequencies more than once in the same radio system so that the total capacity of the system is increased without increasing its allocated bandwidth. Frequency reuse offers the following benefits –

- Allows communications within the cell on a given frequency
- Limits escaping power to adjacent cells
- Allows re-use of frequencies in nearby cells
- Uses the same frequency for multiple conversations
- 10 to 50 frequencies per cell

, Cochannel cells, cochannel interference, Frequency reuse distance, cluster, cluster size

Cochannel cells:

Cochanel cells are cells in a cellular network that use the same frequency channels for communication.

In cellular networks, adjacent cells typically use different frequency channels to avoid interference. However, due to limitations in spectrum availability, cells in different geographic areas may need to share the same frequency channels, leading to cochannel cells.

Cochannel interference:

Cochanel interference occurs when signals from different cells using the same frequency channels interfere with each other.

This interference can degrade the quality of communication and reduce system capacity.

Effective management of frequency allocation and power control helps mitigate cochannel interference in cellular networks.

Frequency reuse distance:

Frequency reuse distance refers to the minimum distance required between cells using the same set of frequencies to avoid interference.

It determines how frequently the same set of frequencies can be reused across a cellular network.

Larger frequency reuse distances allow for more efficient spectrum utilization but may require larger cell sizes.

Cluster:

A cluster in a cellular network refers to a group of cells that share the same set of frequencies and are arranged in a specific pattern.

Clustering allows for efficient frequency reuse within a cellular network while minimizing interference.
Cells within the same cluster typically use the same frequency allocation scheme.

Cluster size:
Cluster size refers to the number of cells within a cluster in a cellular network.
The cluster size determines the spatial distribution of cells sharing the same set of frequencies.
Larger cluster sizes result in fewer clusters but may require larger frequency reuse distances to minimize interference. Conversely, smaller cluster sizes allow for more frequent frequency reuse but may increase the complexity of network planning and management.

2. Classify the wireless networks based on coverage, mobility, and infrastructure.
Based on Coverage:

1. Personal Area Network (PAN): Covers a small area, typically within a few meters. Examples include Bluetooth and Zigbee networks.
2. Local Area Network (LAN): Covers a relatively small geographic area such as a home, office, or campus. Examples include Wi-Fi networks.
3. Metropolitan Area Network (MAN): Covers a larger geographic area such as a city or town. Examples include WiMAX networks.
4. Wide Area Network (WAN): Covers a large geographic area, often spanning across cities, countries, or continents. Examples include cellular networks (3G, 4G, 5G), satellite networks, and long-range Wi-Fi.

Based on Mobility:

1. Fixed Wireless Network: Stationary devices communicate wirelessly within a limited range. Examples include Wi-Fi networks used in homes and offices.
2. Mobile Wireless Network: Devices can move freely while maintaining connectivity. Examples include cellular networks (3G, 4G, 5G) and satellite networks.
3. Nomadic Wireless Network: Devices can move but with limitations. For example, WiMAX networks provide mobility within a city or town but may not support seamless handovers between base stations like cellular networks.

Based on Infrastructure:

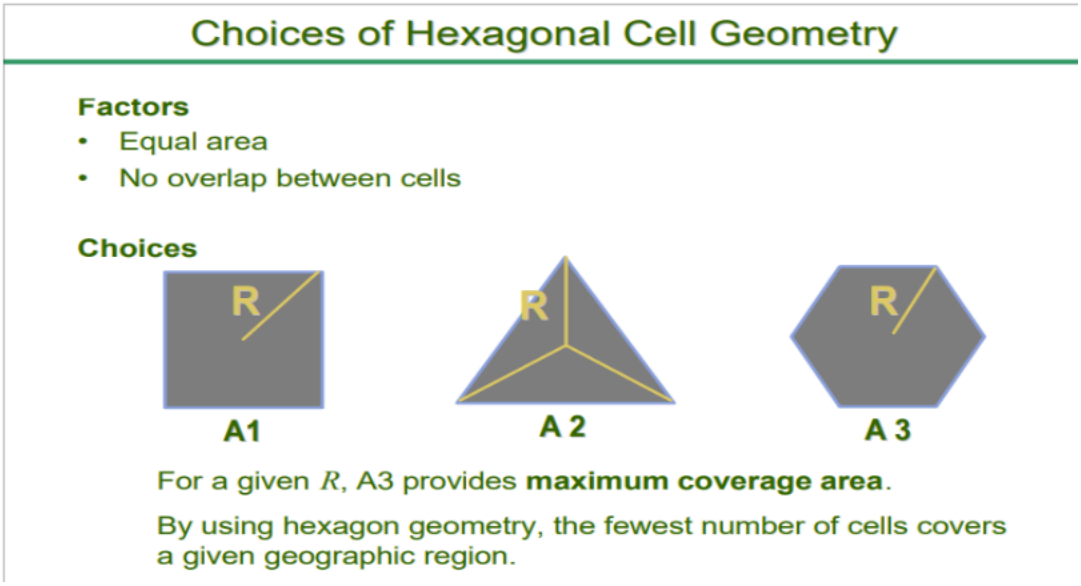
1. Infrastructure-Based Networks: Relies on fixed infrastructure components such as base stations, access points, and routers to facilitate communication. Examples include cellular networks, Wi-Fi networks, and WiMAX networks.

2. Infrastructureless or Ad-Hoc Networks: Devices communicate directly with each other without the need for centralized infrastructure. Examples include mobile ad-hoc networks (MANETs) and wireless sensor networks (WSNs).
3. Hybrid Networks: Combines elements of both infrastructure-based and infrastructure-less networks. For instance, cellular networks use a centralized infrastructure for communication with mobile devices, but devices can also communicate directly with each other in ad-hoc mode when necessary.

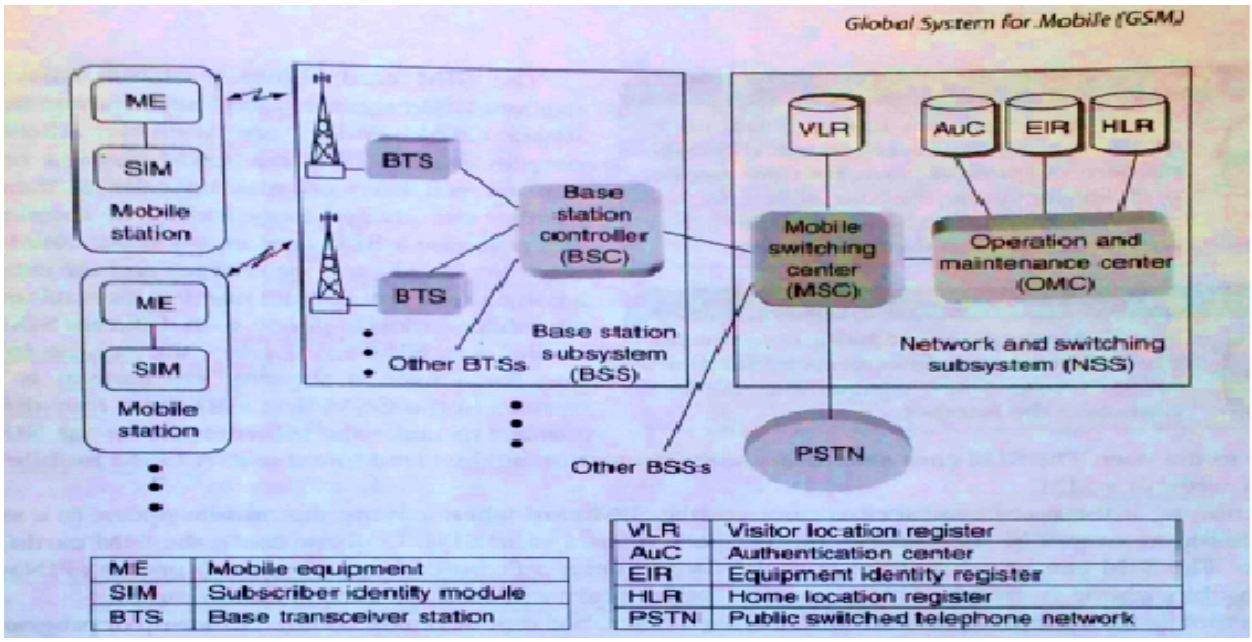
3. List the elements of the cellular system and explain the function of each in brief. Explain the main functions of HLR & VLR in the GSM system.

4. Why is the cell shape considered Hexagonal?

A hexagon cell shape is highly recommended for its easy coverage and calculations.
It offers the following advantages –
Provides equidistant antennas
Distance from center to vertex equals length of side



5. Draw the block diagram of GSM architecture and explain each block in detail.



ME	Mobile equipment
SIM	Subscriber identity module
BTS	Base transceiver station

VLR	Visitor location register
AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
PSTN	Public switched telephone network

ME-

- physical device, consists of Transceiver, Digital Signal Processors and the antenna.
- uniquely identified by the International Mobile Equipment Identity (IMEI).

SIM-

- smart card issued at the subscription time identifying the specification of a user such as a unique number and type of the service.
- The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, service area and other information.
- The SIM card may be protected against unauthorized use by a password or personal identity number (PIN)

BSC:

- is the connection between the mobile station and the Mobile service Switching Center (MSC).
- It is a small switch inside BSS in change of frequency administration, maintains appropriate power levels of signal and handoff among the BTSs inside a BSS. This reduces burden of MSC
- BSC Controller manages the radio resources for one upto several hundred BTSs.

Base Transceiver Station (BTS):

- defines a single cell (radius 100m to 35km)
- BTS components include a Tx, a Rx and signaling equipment to operate over the air interface.
- Interface between BTS & BSC – Abis interface- carries traffics and maintain data
- Interface between BSC & MSC – A interface- standardized within GSM.
- User's speech is converted to 13kbps digitized voice with speech coder –at MS
- Wired network uses 64kbps PCM digitized voice in PSTN technology.

NSS:

- It provides link between cellular networks and PSTN or ISDN or data network.
- The NSS controls handoffs between calls in different BSSs, authenticates users & validates their accounts & includes functions for enabling worldwide roaming of mobile subscriber.
- It include the main switching functions of GSM as well as data based needed for subscriber data and mobility management.
- It consists of
- Mobile Switch Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Center (AuC)
- Equipment Identity Register (EIR)
- Interworking Function (IWF)

MSC:

- It is a hardware part of wireless switch that can communicate with PSTN using Signaling system- 7 (SS-7) protocol.
- It also communicates other MSCs in the coverage area of the service provider.
- Functions of MSC:
    - Call setup, supervision, release and Call routing
    - Digit collection and translation
    - Billing information collection
    - Mobility management (registration, location updating, inter BSS and inter MSC call handoffs)
    - Paging and alerting
    - Management of radio resources during call.
    - Echo cancellation

HLR:

- The HLR represents a central database software that Handles the management of the mobile subscriber account.
- It is referenced using the SS7 signaling capabilities for every incoming call to the GSM network to determine the current location of the subscriber.
- The HLR is kept updated with the current locations of all its mobile subscribers, including those who may have roamed to other network operators within or outside the country.
- The routing information is obtained from the serving VLR on a call-by-call basis, so that for each incoming call the HLR queries the serving VLR for an MSRN(mobile station roaming number).
- Usually, one HLR is deployed for each GSM network for the administration of subscriber configuration and services.
- Besides the up to date information for each subscriber, which is dynamic, HLR maintains the following data on a permanent basis.
- International Mobile Subscriber Identity (IMSI)
- Service subscription information.
- Service restrictions
- Supplementary services subscribed to
- Mobile terminal characteristics
- Billing/ accounting information.

VLR:

- The VLR represents a temporary database software
- Generally there is one VLR per MSC.
- This register contains information about the mobile subscribers who are currently in the service area covered by the MSC/ VLR.
- The VLR also contains information about locally activated features such as call forwarding on busy.

- Thus temporary subscriber information available in VLR includes:
- Features currently activated
- Temporary mobile station identity (TMSI)
- Current location information about the MS.

EIR:

- The EIR is another database that keeps the information about the identity of ME such as IMEI.
- IMEI reveals the details about the manufacturer, country production, and device type.
- This information is used to
    1. prevent calls from being misused
    2. prevent unauthorized or defective MSS
    3. report stolen mobile phones
    4. check if the mobile is operating according to the specification of its type.
- Each ME is identified by IMEI which is memorized by the manufacturer and cannot be removed.
- By the registration mechanisms, the MS always sends IMEI to the network so that the EIR can memorize and assign them to three different lists.
- White list: for all known, good IMEIs- are allowed to enter in the network.
- Black list: for bad or stolen handsets- are not allowed to enter in the network
- Grey list: for handsets/IMEIs that are uncertain- are momentarily not allowed to enter the network eg because a software version is too old or because they are in repair.
- In the future, there will be an interconnection between all the EIRs to avoid the situation where a mobile stolen in one country can be used in a GSM network from a different country.

IWF:

- IWF-is a subsystem in the PLMN (Public Land Mobile Network)
- It allows non speech communications between GSM and other networks.
- The task of IWF is particularly to adopt the transmission parameters and protocol conversion.
- The physical manifestation of an IWF may be through a modem which is activated by MSC dependent on bearer service and destination network.

OSS:

- The implementation of OMC is called the operation and support system (OSS).
- It supports the operation and maintenance of systems and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network.
- OSS supports one or more OMCs (operation maintenance centers)
- Used to monitor & maintain the performance of each MS, BS, BSS, and MSC within the GSM system.
- OSS has main 3 functions:

- To maintain all telecommunication hardware & network operations within a particular service area
- Manage all ME in the sys+tem
- Manage all charging and billing procedures.
- Within each GSM system, an OMC is dedicated to each of these tasks and has a provision for adjusting all base station parameters and billing procedures.
- It provides the ability to determine the performance and integrity of each unit of ME in the system

6. A mobile communication system is allocated a spectrum of 25 MHz and uses an RF channel bandwidth of 25 Khz so that total no of 1000 voice channels are available. a) If the service area is divided into 20 cells with a frequency reuse factor of 4, compute the system capacity.
Total spectrum allocated = 25 MHz
RF channel bandwidth = 25 kHz
Total number of voice channels = 1000
Number of cells = 20
Frequency reuse factor = 4

First, let's calculate the total bandwidth per channel:
Total bandwidth = Total spectrum allocated = 25 MHz = 25,000 kHz
Bandwidth per channel = RF channel bandwidth = 25 kHz

Now, let's calculate the number of channels per cell:
Number of channels per cell = Total bandwidth / Bandwidth per channel
= 25,000 kHz / 25 kHz
= 1000 channels

Since the frequency reuse factor is 4, each cell can use only 1/4th of the available channels. So, the number of channels available per cell for communication = 1000 / 4 = 250 channels.

Now, let's calculate the system capacity:
System capacity = Number of channels per cell × Number of cells
= 250 channels × 20 cells
= 5000 channels

Therefore, the system capacity is 5000 channels.
b) If the cell size is reduced to the extent that the service area is now covered with 100 cells with a frequency reuse factor of 4, compute the system capacity.
Given:

Number of cells = 100
Frequency reuse factor = 4

We already know:
Number of channels per cell = 250 channels (from the previous calculation)

Now, let's calculate the system capacity:
System capacity = Number of channels per cell × Number of cells
= 250 channels × 100 cells
= 25,000 channels

Therefore, with 100 cells covering the service area, each with a frequency reuse factor of 4, the system capacity is 25,000 channels.

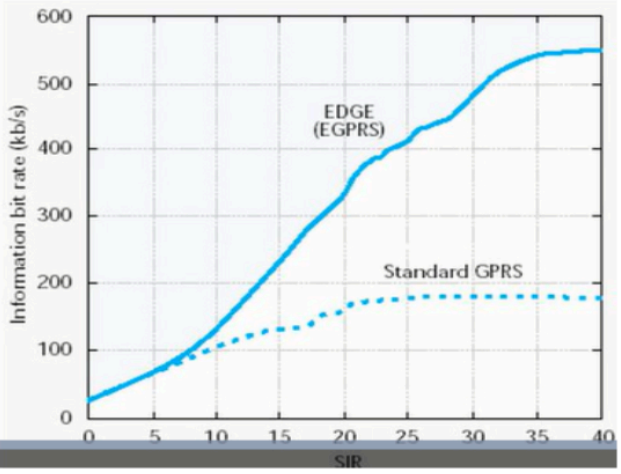
7. Compare and contrast GPRS & EDGE Technology. List their air interface specifications.

GPRS vs EDGE

- EDGE only introduces a new modulation technique and new channel coding that can be used to transmit both packet-switched and circuit-switched voice and data services.
- EDGE is an add-on to GPRS and cannot work alone. And is therefore much easier to introduce than GPRS. GPRS has a greater impact on the GSM system than EDGE has.
- EDGE offers significantly higher throughput and capacity.
- EDGE can transmit three times as many bits as GPRS during the same period of time.
- GPRS can transfer data at rates of 115 kbps theoretically and up to 60 kbps on physical layer,
  whereas EDGE/EGRPS can transfer up to 473.6 kbps and 384 kbps respectively.

- With EDGE, the same time slot can support more users.
- GPRS and EDGE have different protocols and different behaviour on the base station system side.

•On the core network side, GPRS and EDGE share the same packet-handling protocols and, therefore, behave in the same way.
•GPRS and EDGE share the same symbol rate, but the modulation bit rate differs.



Air Interface Specifications:

GPRS Air Interface Specifications:

Modulation: GMSK (Gaussian Minimum Shift Keying)
Coding: Convolutional coding
Maximum Theoretical Data Rate: Up to 114 kbps
Multislot Configurations: Supports up to 8 timeslots (TS) per carrier
Channel Bandwidth: Typically 200 kHz
EDGE Air Interface Specifications:

Modulation: 8-PSK (Eight-Phase Shift Keying)
Coding: Turbo coding
Maximum Theoretical Data Rate: Up to 384 kbps
Multislot Configurations: Supports up to 8 timeslots (TS) per carrier
Channel Bandwidth: Typically 200 kHz

Feature	GPRS	EDGE
Technology Evolution	First-generation packet-switched data technology in GSM networks.	Enhanced version of GPRS, providing higher data rates and spectral efficiency improvements.
Data Rates (Typical)	56 kbps to 114 kbps (real-world: 40-50 kbps)	Up to 384 kbps (real-world: 100-200 kbps)
Modulation	GMSK (Gaussian Minimum Shift Keying)	8-PSK (Phase Shift Keying)
Coding	Convolutional Coding	Turbo Coding
Maximum Theoretical Data Rate	Up to 114 kbps	Up to 384 kbps
Spectral Efficiency	Lower compared to EDGE	Higher compared to GPRS
Frequency Bands	Utilizes GSM frequency bands.	Utilizes GSM frequency bands.

8. What are the two additional components added in GPRS and Edge? List their functions.

SGSN (Serving GPRS Service Node):

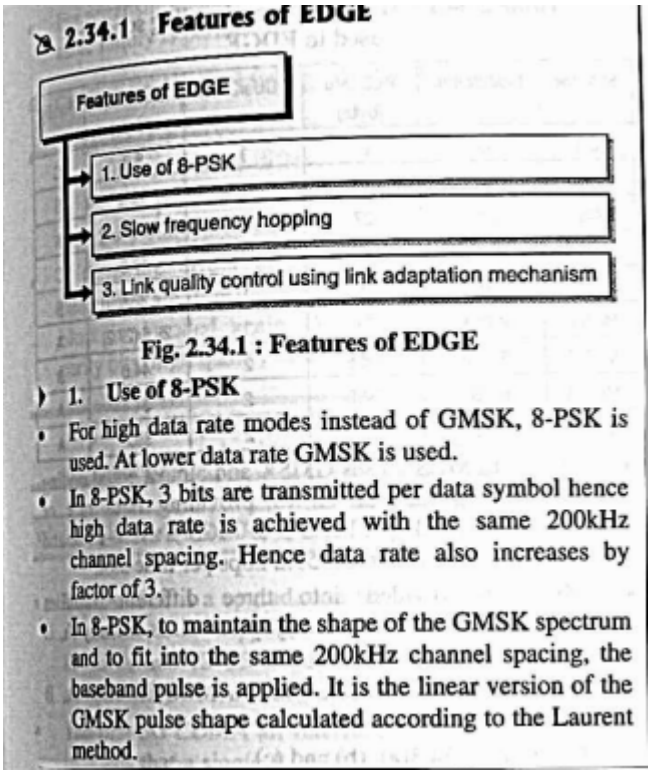
- It provides a variety of services to the mobiles:
- Packet routing and transfer
- Mobility management
- Authentication
- Attach/detach
- Logical link management
- Charging data
- There is a location register within the SGSN and this stores location information (e.g., current cell, current VLR). It also stores the user profiles (e.g., IMSI, packet addresses used) for all the GPRS users registered with the particular SGSN.

GGSN (Gateway GPRS Service Node)

- The GGSN organizes the inter-working between the GPRS / EDGE network and external packet switched networks to which the mobiles may be connected. These may include both Internet and X.25 networks.
- The GGSN can be considered to be a combination of a gateway, router and firewall as it hides the internal network to the outside.

- When the GGSN receives data addressed to a specific user, it checks if the user is active, then forwarding the data. In the opposite direction, packet data from the mobile is routed to the right destination network by the GGSN.

9. What are the new features added in EDGE Technology to get higher data rates?

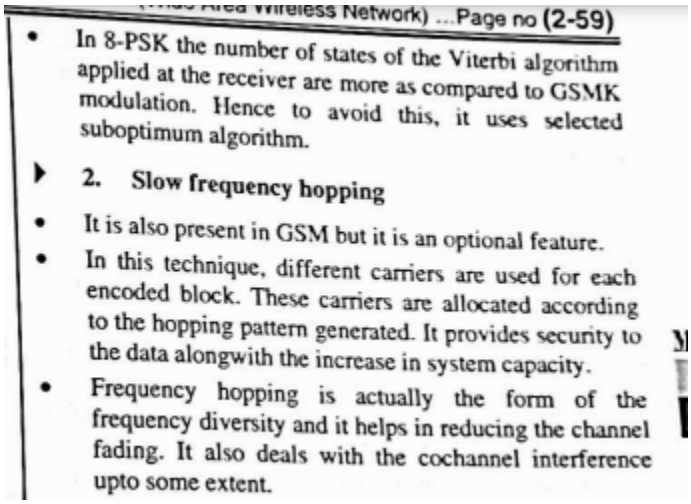


2.34.1 Features of EDGE

Fig. 2.34.1 : Features of EDGE

1. **Use of 8-PSK**

- For high data rate modes instead of GMSK, 8-PSK is used. At lower data rate GMSK is used.
- In 8-PSK, 3 bits are transmitted per data symbol hence high data rate is achieved with the same 200kHz channel spacing. Hence data rate also increases by factor of 3.
- In 8-PSK, to maintain the shape of the GMSK spectrum and to fit into the same 200kHz channel spacing, the baseband pulse is applied. It is the linear version of the GMSK pulse shape calculated according to the Laurent method.



...Page no (2-59)

- In 8-PSK the number of states of the Viterbi algorithm applied at the receiver are more as compared to GSMK modulation. Hence to avoid this, it uses selected suboptimum algorithm.

2. **Slow frequency hopping**

- It is also present in GSM but it is an optional feature.
- In this technique, different carriers are used for each encoded block. These carriers are allocated according to the hopping pattern generated. It provides security to the data alongwith the increase in system capacity.
- Frequency hopping is actually the form of the frequency diversity and it helps in reducing the channel fading. It also deals with the cochannel interference upto some extent.

The new features added in Enhanced Data Rates for GSM Evolution (EDGE) technology, also known as Evolved EDGE or 2.875G, aim to increase data rates and reduce latencies compared to the original EDGE standard. These enhancements include:

- Lowered Transmission Time Interval: The time interval between transmissions is halved from 20 ms to 10 ms, which significantly reduces latencies.
- Increased Bit Rates: The peak bandwidth can reach up to 1 Mbit/s, with real-world downlink speeds of up to 600 kbit/s.
- Higher Symbol Rate and Modulation Schemes: The use of dual carrier, higher symbol rate, and higher-order modulation (32QAM and 16QAM instead of 8PSK) contributes to increased data rates.
- Turbo Coding: This technique improves error correction, further enhancing the reliability of data transmission.
- Dual Antennas: Improved signal quality through the use of dual antennas, which enhances average bit rates and spectrum efficiency.

10. Name the modulation scheme used in EDGE? What is the advantage of using it?

EDGE (Enhanced Data Rates for GSM Evolution) uses a modulation scheme known as 8PSK (8 Phase Shift Keying).

The advantage of using 8PSK in EDGE over the GMSK (Gaussian Minimum Shift Keying) used in GSM and GPRS is that 8PSK encodes three bits of data per symbol, compared to GMSK's one bit per symbol.

This essentially triples the data rate for a given bandwidth, allowing for higher data transfer rates compared to GPRS.

11. Define one-time slot and one superframe structure used in GSM.

One-Time Slot: A GSM time slot is the smallest unit of time in the GSM system, with a duration of 576.92 µs (microseconds) .Each time slot is allocated a specific frequency for communication, allowing for multiple time slots to be used simultaneously within the same frame to increase the data rate and capacity of the system. There are 156.25 bits per time slot, with each bit being 3.69231 µs long, enabling high-speed data transmission.

One Superframe Structure: A superframe in GSM is a larger time unit that contains 1326 TDMA (Time Division Multiple Access) frames, equating to a total duration of 6.12 seconds. The superframe can either carry 51 of 26-Multiframes or 26 of 51-Multiframes, providing flexibility in how data is organized and transmitted over time. Each of these frames is 4.61538 ms long, and within each frame, there are 8 time slots as previously described . This structure allows for efficient use of the available spectrum and supports the high data rates required by GSM networks.

12. What is incremental redundancy in EDGE?

Incremental Redundancy in EDGE (Enhanced Data rates for GSM Evolution) is a technique used to improve the reliability and efficiency of data transmission over the

air interface. In EDGE, data packets are transmitted with additional redundancy bits in a progressive manner, providing adaptive error correction capabilities.

Here's how incremental redundancy works in EDGE:

Initial Transmission: When a data packet is transmitted, it includes a certain amount of redundancy in the form of error correction coding. This redundancy allows the receiver to detect and correct errors that may occur during transmission.

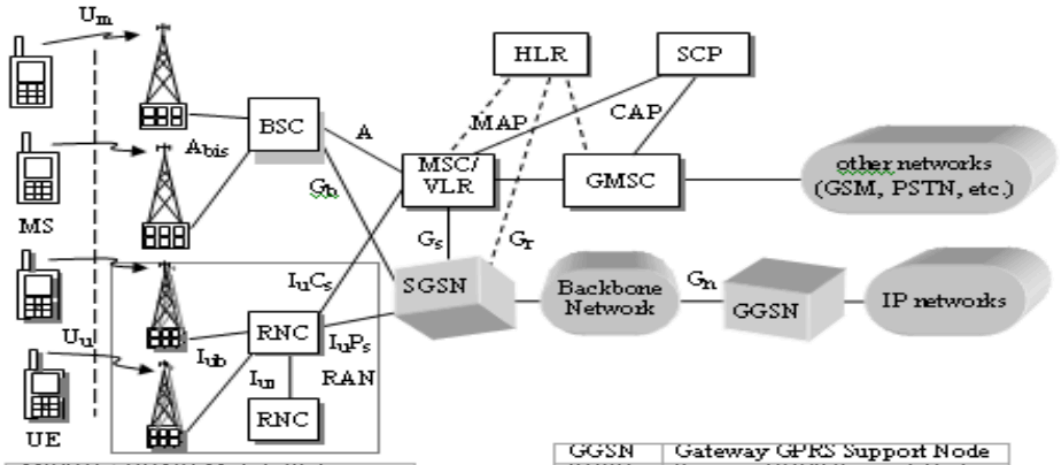
Request for Additional Redundancy: If errors are detected at the receiver, instead of requesting a retransmission of the entire data packet, the receiver can request only the additional redundancy bits needed to correct the errors. This request is sent back to the transmitter.

Progressive Redundancy: Upon receiving the request from the receiver, the transmitter sends only the requested additional redundancy bits, rather than retransmitting the entire packet. These additional redundancy bits are sent incrementally, providing finer granularity in error correction.

Adaptive Error Correction: The receiver combines the initially received data packet with the additional redundancy bits received in response to its request. By combining the two sets of information, the receiver can correct errors more effectively, even in the presence of varying channel conditions.

13. With reference to UMTS, draw the network architecture and list the functions of RNC & nodeB.

UMTS Network Architecture



MS/UE	2G/3G Mobile Station
RAN	Radio Access Network
CAP	CAMEL Application Part
GMSC	Gateway MSC

GGSN	Gateway GPRS Support Node
SGSN	Serving GPRS Support Node
BS/NB	2G/3G Base Station
RNC	Radio Network Controller
MAP	Mobile Application Part

105

UTRAN Architecture

3G

• RNS has main two elements : 1) Node B 2) RNC

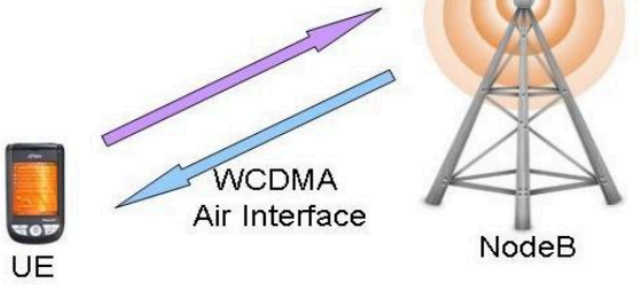
1. Radio Network Controller (RNC):

Functions:

- Radio resource management
- Serving RNS relocation
- Frame synchronization
- Macro diversity combining
- Intra-UTRAN handoff
- Splitting of the I_{ub} data streams
- Outer loop power control
- RLC sublayers function execution

• Functions equivalent to BSC in GSM

• RNCs can manage handovers without using MSC and SGSN



2. Node B

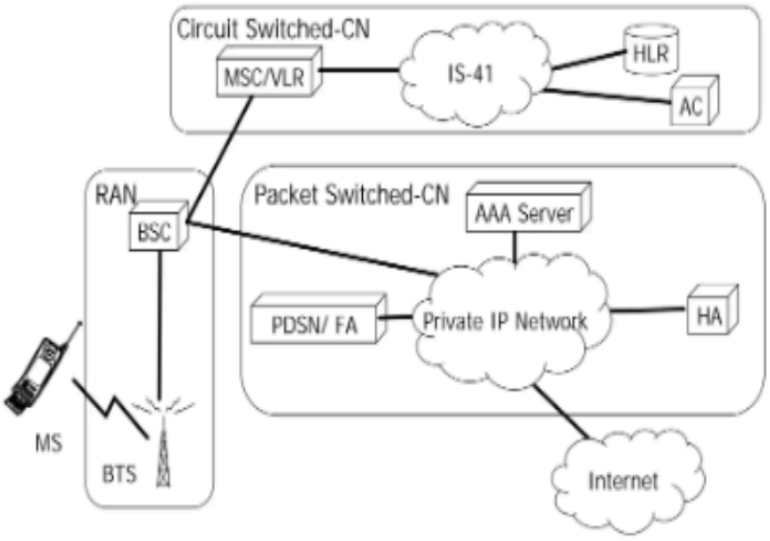
• equivalent to BTS

• physically co-located with GSM BTS to reduce the cost

108

14. With reference to CDMA 2000, draw the network architecture and explain how it is different from UMTS.

cdma2000 Network Architecture



- AAA: Authentication, Authorization and Accounting
- FA: Foreign Agent
- GR: Gateway Router
- HA: Home Agent
- PDSN: Packet Data Serving Node

Air Interface Parameters (1)

	UMTS	cdma2000
Spreading rate	**3.84 Mcps**	**1.2288 Mcps**
Bandwidth	**5 MHz**	**1.25 MHz**
Synchronization between cell sites	**Asynchronous**	**Synchronous**
Configuration	**Direct spread configuration**	**Direct spread (1x) Multi-carrier (3x forward link)**
Channel coding	**Convolutional Turbo (Parameters flexible)**	**Convolutional Turbo (Parameters fixed in the standard)**

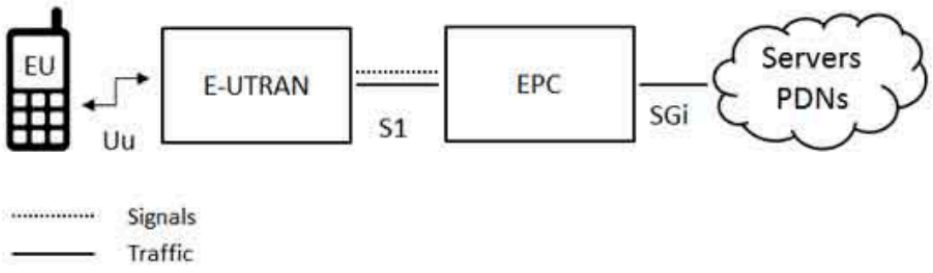
Air Interface Parameters (2)

	UMTS	cdma2000
Modulation	QPSK in both directions	QPSK in forward BPSK in reverse
Frame size	10 msec for physical layer 10,20,40 and 80 msec for transport layer	5 (for signaling), 20, 40 and 80 msec physical layer frames
Modes	FDD and TDD Mode	Only FDD Mode
Transmit Diversity schemes	Time Switched Transmit Diversity Space Time Block Coded Transmit Diversity	Orthogonal Transmit Diversity Space Time Spreading

15. Draw the network architecture of LTE and explain the functions of each component in brief.

The high-level network architecture of LTE is comprised of following three main components:

The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:



1. **The User Equipment (UE).**

The User Equipment (UE)

The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME). The mobile equipment comprised of the following important modules:

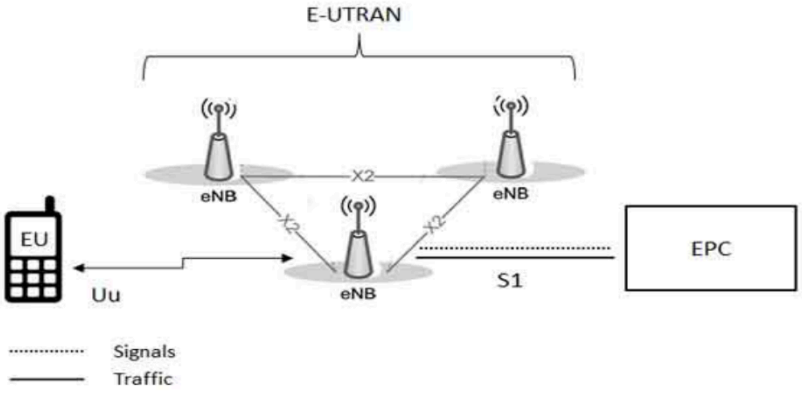
- **Mobile Termination (MT)** : This handles all the communication functions.
- **Terminal Equipment (TE)** : This terminates the data streams.
- **Universal Integrated Circuit Card (UICC)** : This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM).

A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

2. **The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).**

The E-UTRAN (The access network)

The architecture of evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated below.



The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:

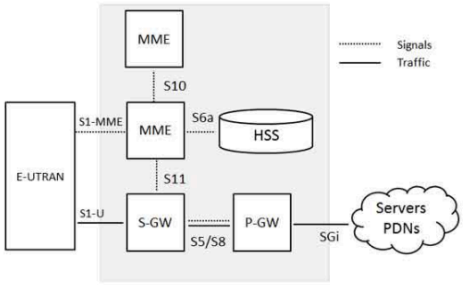
- The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

- Each eBN connects with the EPC by means of the S1 interface and it can also be connected to nearby base stations by the X2 interface, which is mainly used for signalling and packet forwarding during handover.
- A home eNB (HeNB) is a base station that has been purchased by a user to provide femtocell coverage within the home.
- A home eNB belongs to a closed subscriber group (CSG) and can only be accessed by mobiles with a USIM that also belongs to the closed subscriber group.

3. The Evolved Packet Core (EPC).

The Evolved Packet Core (EPC) (The core network)

- There are few more components which have not been shown in the diagram to keep it simple. These components are like the Earthquake and Tsunami Warning System (ETWS), the Equipment Identity Register (EIR) and Policy Control and Charging Rules Function (PCRF).



2G/3G Versus LTE

Following table compares various important Network Elements & Signaling protocols used in 2G/3G abd LTE.

2G/3G	LTE
GERAN and UTRAN	E-UTRAN
SGSN/PDSN-FA	S-GW
GGSN/PDSN-HA	PDN-GW
HLR/AAA	HSS
VLR	MME
SS7-MAP/ANSI-41/RADIUS	Diameter
DiameterGTPc-v0 and v1	GTPc-v2
MIP	PMIP

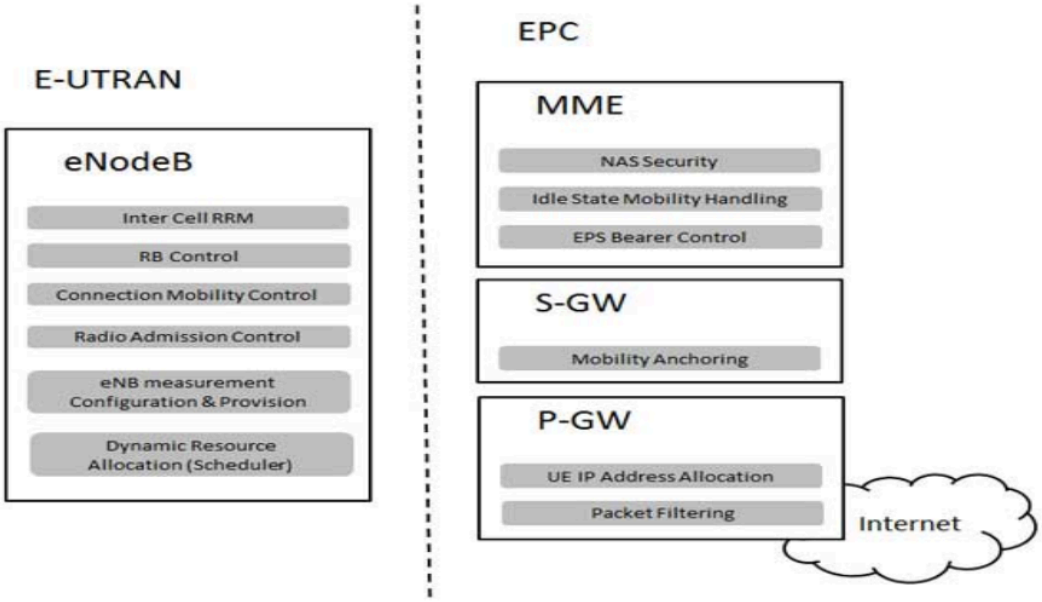
- The Home Subscriber Server (HSS) component has been carried forward from UMTS and GSM and is a central database that contains information about all the network operator's subscribers.
- The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN). The PDN gateway has the same role as the GPRS support node (GGSN) and the serving GPRS support node (SGSN) with UMTS and GSM.

- The serving gateway (S-GW) acts as a router, and forwards data between the base station and the PDN gateway.
- The mobility management entity (MME) controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS).
- The Policy Control and Charging Rules Function (PCRF) is a component which is not shown in the above diagram but it is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW.

- The interface between the serving and PDN gateways is known as S5/S8. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

Functional split between the E-UTRAN and the EPC

Click



16. Write short notes on LoRA and LoRAWAN.

Most communication radios like Zigbee, BLE, WiFi among others are of short range and others like 3G and LTE, are power hungry and the span of their coverage areas cannot be guaranteed especially in developing countries.
This is where LoRa comes in.

• LoRa(which stands for Long Range) is a patented wireless communication technology that combines ultra-low power consumption with an effective long range.
• While range highly depends on the environment and possible obstructions (LOS or N-LOS), LoRa typically has a range between 13-15Km, which means a single LoRa gateway can provide coverage for an entire city, and with a couple more, a whole country.
• The technology was developed by Cycleoin France and came to fore when the company was acquired by Semtechin 2012. We used LoRa module with Arduino and with Raspberry Pi and they worked as expected.

A LoRa radio comprises a few features that help it achieve long-range effective power and Low cost.
Some of these features include;
• Modulation Technique
• Frequency
• Adaptive Data Rates
• Adaptive PowerLevels

Advantages of LoRa
1. Long Range and Coverage: With up to 15km LOS Range, its range can't be compared with that of any other Communication protocol.
2. Low Power: LoRa offers hyper low power radios which makes them Ideal for devices that are required last for 10 years or more on a single battery charge.
3. Low-cost hardware: Infrastructures for LoRaWAN are extremely low cost compared to other networks and the cost of radios for end-devices is equally Low. More so, several open-source versions of infrastructures like gateways are being developed which helps to reduce costs further1
4. High Capacity: Thousands of end devices could be connected to a single LoRa gateway

Disadvantages of LoRa
With a maximum data rate of around 50kb/s, LoRa has the lowest of data rates when compared with most of the other technology which makes it not ideal for certain applications where high data rates are required.

LoRaWAN
• LoRaWAN is a high capacity, Long Range, open, Low Power Wide Area Network (LPWAN) standard designed for LoRa Powered IoT Solutions by the LoRa Alliance.
• It is a bi-directional protocol that takes full advantage of all the features of the LoRa technology to deliver services including reliable message delivery, end-to-end security, location, and multicast capabilities.
• The standard ensures the interoperability of the various LoRaWAN networks world-wide.
• There is usually a mix up when people try to define LoRa and LoRaWAN which is probably best solved by examining the OSI reference stack Model.

• Simply put, based on the OSI stack Model, LoRaWAN corresponds to Media Access protocol for the communication network while LoRa corresponds to the Physical layer.
• Thus LoRaWAN defines the communication protocol and system architecture for the network, while LoRa architecture enables the long-range communication link.

• The two of them merged together to provide the functionality that determines battery life of a node, the network capacity, the quality of service, the security and other applications served by the network.
• While LoRaWAN is the most popular MAC layer for LoRa other proprietary layers which are also built on the LoRa technology exists.
• A good example is Symphony link by Link Labs which is specially developed for industrial applications.

• Opposed to the mesh network topology adopted by most networks, LoRaWAN uses the star network architecture, thus, rather than have each end-device in an almost always on state, repeating transmission from other devices to increase range, end-devices in the LoRaWAN network communicate directly with gateways and are only on when they need to communicate with the gateway since range is not a problem.
• This is a contributing factor to the Low power features and High battery life obtained in the LoRa end devices

Assignment 3

1. Explain basic configuration of wireless LAN Network.(phind)
Configuring a basic wireless LAN (WLAN) network involves several key steps to ensure a reliable and secure connection. Here's a simplified guide based on the provided sources:
Design and Survey: Before starting the configuration, it's crucial to design your network based on a survey of your environment. This step helps in determining the best placement for your wireless access points (APs) and ensuring optimal coverage. A proper design can prevent costly rework and ensure a reliable connection.
Implement WLAN Components: This step involves the actual setup of your wireless network. It includes configuring the APs, setting up security measures (like Extensible Authentication Protocol (EAP), RADIUS servers, and encryption), and adjusting radio-specific settings such as power and channel. For the 2.4 GHz band, it's recommended to stick with channels 1, 6, and 11 to minimize co-channel interference. In the 5 GHz band, avoid using 80 or 160 MHz channels unless necessary, and be cautious with high power settings as they can cause more issues than they solve. Ensure your switch infrastructure and Power over Ethernet (PoE) capabilities match the Wi-Fi radio technology in use.
Basic Wireless LAN Connection Configuration: This involves setting up the client devices to connect to the wireless network. You need to ensure that the drivers for the wireless client cards are installed. Then, configure the Service Set Identifier (SSID), authentication method, and encryption settings on both the AP and the client devices. For example, you can use open authentication with Wired Equivalent Privacy (WEP)

encryption for basic setups, but it's recommended to use more secure methods for sensitive networks.

Integrations: The wireless network is part of a larger network environment, including switch ports, Dynamic Host Configuration Protocol (DHCP) server settings, and firewall rules. Ensure that these components are correctly configured to support your WLAN. This might require coordination among different staff members or departments.

Testing and Optimization: After setting up the network, test the connection for reliability and performance. This includes checking the signal strength, data rates, and ensuring that devices can connect and communicate without issues. Based on the test results, you may need to adjust the configuration, such as changing channels or increasing the power of the APs.

2. Define BSS and ESS and explain their role in the architecture.

Basic service set configuration

- ✔ It relies on an AP that acts as the logical server for a single WLAN cell or channel
- ✔ Communications between station 1 and station 4 actually flow from station 1 to AP1 and then from AP1 to AP2 and then from AP2 to AP4 and finally AP4 to station 4 (refer to Figure 21.4).
- ✔ An AP performs a bridging function and connects multiple WLAN cells or channels and connects WLAN cells to a wired enterprise LAN.

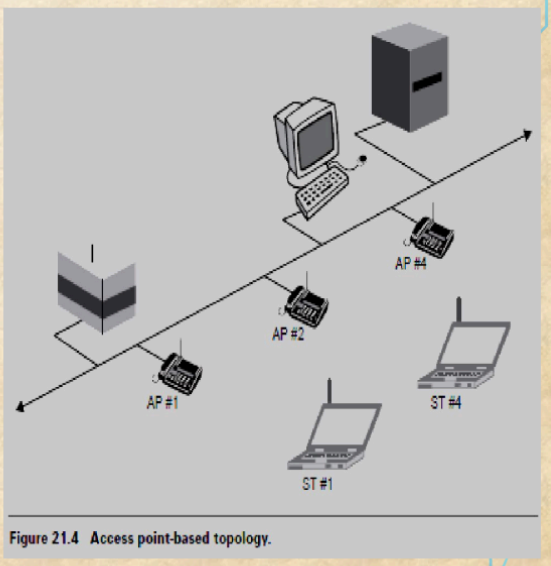
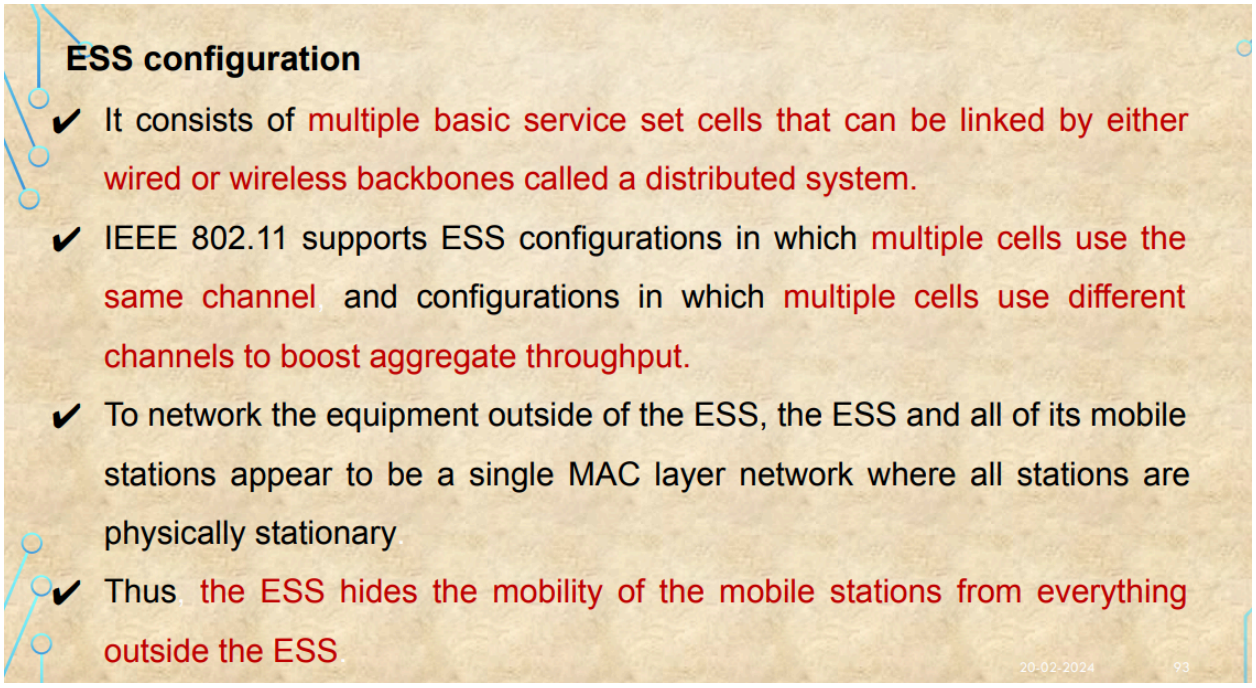


Figure 21.4 Access point-based topology.



3. Draw and explain the protocol stack for IEEE 802.11 (phind)

The IEEE 802.11 protocol stack, commonly known as Wi-Fi, is a set of standards for wireless LAN (WLAN) technology. It defines the MAC (Media Access Control) and physical layer specifications for connecting devices in a LAN without cables, using high-frequency radio waves. The architecture supports both wired and wireless connections, allowing seamless integration with other networks like 2G, 3G, and 4G. The 802.11 family consists of various specifications and amendments, including 802.11a, 802.11b, 802.11e, 802.11g, 802.11n, and more recent standards like 802.11ac, 802.11ax, etc.

The protocol stack for IEEE 802.11 can be broken down into several layers:

Physical Layer (PHY): This layer is responsible for the transmission and reception of raw bit streams over the air or through a cable. It defines the modulation and coding schemes, frequency bands (e.g., 2.4 GHz, 5 GHz), and channel specifications.

Media Access Control (MAC): The MAC layer manages how devices in a network gain access to the medium and permission to transmit. It defines how to identify devices, manage data transmission, and resolve collisions.

Logical Link Control (LLC): This layer provides flow control and error checking to ensure reliable data transmission. It uses the LLC sublayer to multiplex different data types onto the MAC layer.

Network Layer (NET): The network layer handles packet forwarding, including routing and network addressing. It uses the logical addressing scheme defined by the Internet Protocol (IP).

Data Link Layer (DAT): This layer provides error-free data transfer between two nodes and manages frame synchronization, flow control, and error checking.
Physical Layer Convergence Protocol (PHY-CONV): This layer provides a means for the MAC layer to communicate with the physical layer.

The IEEE 802.11 architecture supports two primary modes of operation:
Infrastructure Mode (BSS): In this mode, wireless clients (STAs) communicate with an access point (AP) that acts as a bridge to a wired network (DS). The AP can be part of an Extended Service Set (ESS), which is a collection of multiple BSSs.
Independent Basic Service Set (IBSS): Also known as Ad-Hoc mode, this mode allows devices to communicate directly with each other without the need for an access point. Each device in an IBSS acts as both a client and an access point.

The frame format for IEEE 802.11 includes several fields such as Frame Control, Duration, Address fields (Source, Destination, and BSSID), Sequence Control, Data, and Frame Check Sequence (FCS) for error detection.

The IEEE 802.11 standards have evolved over time to support higher data rates, improved security, and better performance in various environments. Each generation of the standard, such as 802.11n and 802.11ac, introduces enhancements like MIMO (Multiple Input Multiple Output) technology, which allows for multiple simultaneous data streams to improve throughput and range

4. Explain the operating principle of OFDM used for IEEE 802.11a .(phind)
Orthogonal Frequency-Division Multiplexing (OFDM) is a digital transmission method used in various applications, including IEEE 802.11a, a wireless LAN (WLAN) standard that operates in the 5 GHz frequency band.
The operating principle of OFDM for IEEE 802.11a involves several key components and steps:
Data Encoding: The incoming bitstream representing the data to be sent is divided into multiple streams. These streams are then modulated onto multiple closely spaced orthogonal subcarrier signals. This allows multiple bits to be transmitted in parallel, significantly improving the efficiency of data transmission.
Modulation Schemes: Each subcarrier is modulated with a conventional modulation scheme, such as Quadrature Amplitude Modulation (QAM), at a low symbol rate. This approach maintains total data rates similar to those of conventional single-carrier modulation schemes in the same bandwidth.
Orthogonality and Subcarrier Frequencies: A key feature of OFDM is the orthogonality of the subcarrier signals. This means that the subcarriers are chosen so that they are orthogonal to each other, eliminating crosstalk between sub-channels and simplifying the design of both the transmitter and receiver. The orthogonality also

allows for high spectral efficiency, with a total symbol rate near the Nyquist rate for the equivalent baseband signal, enabling almost the entire available frequency band to be used.

Guard Interval and Inter-Symbol Interference: The introduction of a guard interval between symbols allows for the elimination of intersymbol interference (ISI) and the use of echoes and time-spreading to achieve a diversity gain, i.e., a signal-to-noise ratio improvement. This mechanism also supports the design of single frequency networks (SFNs) where several adjacent transmitters send the same signal simultaneously at the same frequency.

Demodulation: The demodulation process at the receiver side is based on Fast Fourier Transform (FFT) algorithms. This allows for the efficient reconstruction of the original data from the received subcarriers.

PLCP Preamble and Header: In the context of IEEE 802.11a, the Physical Layer Convergence Procedure (PLCP) is used to convert the PHY Sublayer Service Data Units (PSDU) into a Protocol Data Unit (PPDU) for transmission. The PPDU includes a PLCP preamble and header, which are processed at the receiver to aid in demodulation and delivery of the PSDU. The PLCP preamble consists of 12 symbols, with specific subcarriers used for training and estimating the frequency and channel.

Data Transmission: The data portion of the packet is transmitted at the data rate indicated in the signal field of the PLCP header. The transmission medium is wireless, and the operating frequency band is 5 GHz. The OFDM of the 802.11a system supports data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, with mandatory support for transmitting and receiving at data rates of 6, 12, and 24 Mbps.

5. Explain the architecture of wireless LAN Network with suitable diagram.

3.3 IEEE 802.11 (WI-FI)

In the family of IEEE 802.11 many WLAN standards are included. The main goal of this standard is to set up simple and robust WLAN which offers time- bounded and asynchronous services.

Syllabus Topic : IEEE 802.11(Wi-Fi) – Architecture

3.3.1 System Architecture of IEEE 802.11

GQ. Explain different architectures of WLAN.

Wireless networks can exhibit two different basic system architectures.

A. Infrastructure based WLAN
B. Ad hoc WLAN

3.3.1(A) Infrastructure based WLAN Architecture

- Refer Fig. 3.3.1. It shows the system architecture of WLAN.

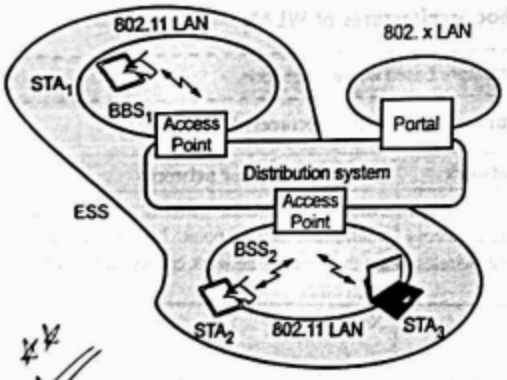


Fig. 3.3.1 : WLAN system architecture

The system comprises of

(i) STA (Station)
(ii) Access Point (AP)
(iii) Portal (PO)
(iv) DS (Distribution System)
(v) BSS (Basic Service Set)
(vi) ESS (Extended Service Set)

(i) STA (Station)

It is nothing but a mobile station.

(ii) Access Point (AP)

- It is a special central traffic relay station that usually operates on fixed channel.
- It is stationary. It can be viewed as the coordinator in the group of stations.
- It is like the base station in GSM network.
- It supports roaming that is changing access points. They also control power management and synchronization functions.

(iii) Portal (PO)

- It is typical access point which interconnects wired LAN and wireless LAN.
- It is the logical interconnection between the two networks.

(iv) DS (Distribution System)

- DS is the backbone network that is responsible for the MAC layer transport of MAC service data units.
- Examples include 802.3 Ethernet, IEEE 802.4 token bus LAN, fiber optic LAN etc.
- A DS connects several BSSs via the AP to form a single network. Thus, it extends the wireless coverage area.
- It handles data transfer between the different APs.

(v) BSS (Basic Service Set)

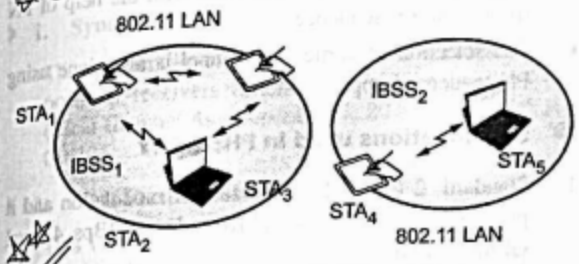
- It is the smallest building block of the WLAN system.
- It consists of some number of stations and access points in the network.
- Simplest BSS has only two STAs.
- The association of STA and BSS is entirely dynamic.
- BSS may be isolated, or it may be connected to the backbone Distribution System (DS) through an Access Point (AP).
- This mode of operation is known as ad hoc networking as this type of IEEE 802.11 WLAN is created and maintained without prior administrative arrangement.

(vi) ESS (Extended Service Set)

- It is a set of two or more BSSs forming a single sub-network.
- ESS configurations consist of multiple BSS cells that can be linked by either wired or wireless backbones known as DS.
- IEEE 802.11 supports ESS configurations in which multiple cells use the same channel.
- It may also use different channel to aggregate throughput.

- The STAs in ESS can be mobile or stationary.
- Stationary STAs are actually AP. They are part of wired LAN.
- When the BSSs are connected, two stations can communicate directly without AP.
- But if stations are belonging to different BSSs then they have to communicate via AP.

3.3.1(B) Ad hoc WLAN Architecture



(SD4) **Fig. 3.3.2 : ad-hoc WLAN architecture**

- Refer Fig. 3.3.2. It shows ad hoc WLAN architecture.
- In addition to infrastructure-based architectures, IEEE 802.11 also supports ad hoc network between stations.
- It forms IBSS (Independent Basic Service Set).

IBSS (Independent Basic Service Set)

- When all the stations in BSS are mobile and it has no connection with other BSSs, the BSS is known as IBSS.
- It is an ad hoc network. This does not contain AP and it cannot transmit data to other stations.
- It is formed using one or more stations belonging to same radio frequency. The stations within the IBSS can communicate directly without APs.
- Several IBSS can be formed by keeping certain distance between them or by using different carrier frequencies.

6. Compare IEEE 802.11DSSS and IEEE 802.11FHSS.

Category	FHSS	DSSS
Abbreviation	FHSS is Frequency-Hopping Spread Spectrum	DSSS is Direct-Sequence Spread Spectrum
Definition	FHSS is a type of spread spectrum technology in which the frequency of the transmitted signal changes according to a specific pattern.	DSSS is a type of spread spectrum technology in which the transmitted signal is spread across multiple frequency bands.
Pattern	In FHSS, the data transmission is encoded and decoded using a specific pattern called **hopset**.	In DSSS, the data transmission is encoded and decoded using a pseudo-random binary sequence or **chip** code.
Frequency band	FHSS transmits data using a narrowband carrier that hops among different frequency channels.	DSSS transmits data using a wider frequency band.
Interference resistant	FHSS is more resistant to interference because it uses frequency hopping, which makes it difficult to intercept the signal.	DSSS is more vulnerable to interference because it uses a wider frequency band.
Susceptibility	FHSS is less susceptible to multipath fading, it is a phenomenon in which the transmitted signal arrives at the receiver via multiple paths, resulting in a loss of signal quality.	DSSS is more susceptible to multipath fading because it uses a wider frequency band.
Transmission speed	FHSS has low transmission rates (up to 3 Mbps).	DSSS has high transmission rates (up to 11 Mbps).
Modulation techniques used	Multilevel Frequency Shift Keying (FSK) was used.	BPSK (Binary Phase-Shift Keying) was used.
Efficiency	FHSS is generally more efficient than DSSS in terms of bandwidth utilization.	DSSS is less efficient because it uses a wider frequency band.
Application areas	It is widely used in a variety of applications, including wireless networking like Bluetooth, mobile communications, and military communications.	It is well-suited for particular applications where the signal must travel over long distances like GPS, and WIFI.

7. Explain the frame structure of IEEE 802.11DSSS / IEEE 802.11FHSS.

DSSS PHY

In the DSSS PHY, data transmission over the media is controlled by the physical medium dependent (PMD) sublayer as directed by the physical layer convergence procedure (PLCP) sublayer. The PMD sublayer takes the binary information bits from the PLCP protocol data unit (PPDU) and converts them into RF signals by using modulation and DSSS techniques.

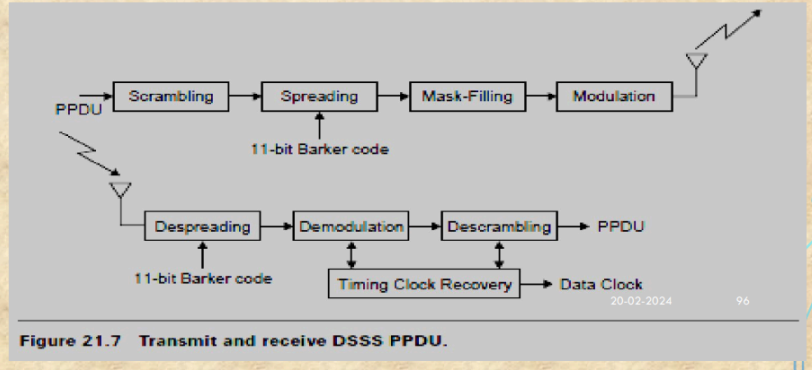
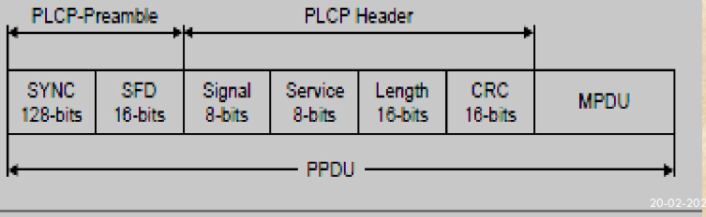


Figure 21.7 Transmit and receive DSSS PPDU.

- ✔ Figure shows the PPDU frame, which consists of a PLCP preamble, PLCP header, and MAC protocol data unit (MPDU).
- ✔ The PLCP preamble and PLCP header are always transmitted at 1 Mbps, and the MPDU can be sent at 1 or 2 Mbps.
- ✔ The **start of frame delimiter (SFD)** contains information that marks the start of the PPDU frame. The ***signal field*** indicates which modulation scheme should be used to receive the incoming MPDU. The binary value in this field is equal to the data rate multiplied by 100 kbps.

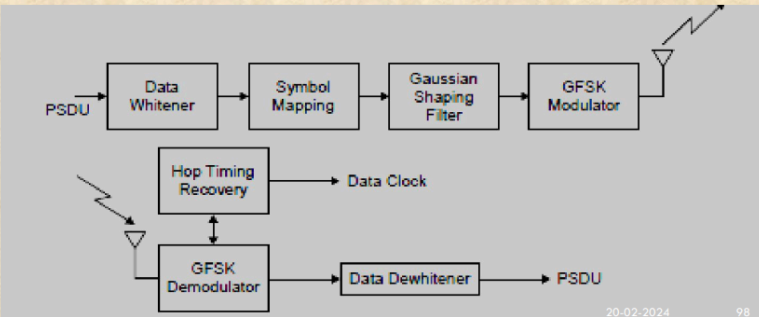


20-02-2024 97

Figure 21.8 DSSS PHY PPDU frame.

FHSS PHY

- In FHSS PHY, data transmission over media is controlled by the FHSS physical medium dependent (PMD) sublayer as directed by the FHSS PLCP sublayer
- The FHSS PMD takes the binary information bits from the whitened PSDU and converts them into RF signals by using carrier modulation and FHSS techniques (see Figure 21.10).



20-02-2024 98

Figure 21.10 FHSS PHY transmitter and receiver.

- PPDU consists of: PLCP preamble, PLCP header, PLCP service data unit (PSDU).
- The PLCP preamble is used to acquire the incoming signal and synchronize the receiver's demodulator.
- The PLCP header contains information about PSDU from the sending physical layer. The PLCP preamble and header are transmitted at 1 Mbps.
- The *sync field* contains a string of alternating 0s and 1s pattern and is used by the receiver to synchronize the receiver's packet timing and correct for frequency offsets.

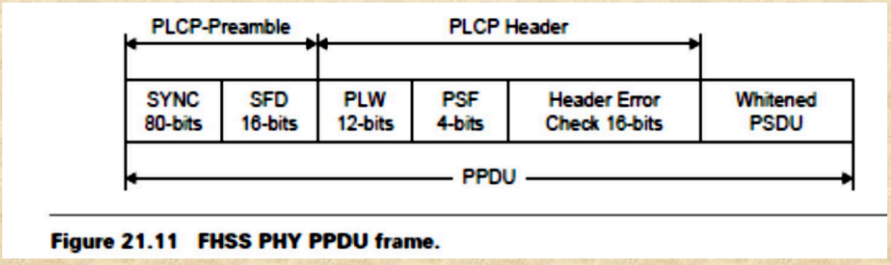


Figure 21.11 FHSS PHY PPDU frame.

8. Explain back off algorithm.

- used to resolve contention problems among different stations wishing to transmit data at the same time.
- When a station goes into the backoff state, it waits an additional, randomly selected number of time slots.
- During the wait, the station continues sensing the medium to check whether it remains free or another transmission begins.
- At the end of its contention window, if the medium is still free the station can send its frame.
- If during the contention window another station begins transmitting data, the backoff counter is frozen and counting down starts again when the channel returns to the idle state.

- There is a problem related to the CW dimension.

- With a small CW, if many stations attempt to transmit data at the same time it is very possible that some of them may have the same backoff interval. This means that there will continuously be collisions, with serious effects on the network performance.

- On the other hand, with a large CW, if few stations wish to transmit data they will likely have long backoff delays resulting in the degradation of the network performance. The solution is to use an exponentially growing CW size.

- It starts from a small value (CWmin =31) and doubles after each collision, until

it reaches the maximum value CWmax (CWmax =1023).

In 802.11 the backoff algorithm must be executed in three cases:

1. When the station senses the medium is busy before the first transmission of a packet

2. After each retransmission

3. After a successful transmission

- This is necessary to avoid a single host wanting to transmit a large quantity of data, occupying the channel for too long a period, and denying access to all other stations.

- The backoff mechanism is not used when the station decides to transmit a new packet after an idle period and the medium has been free for more than the DIFS (see Figure 21.14).

9. Explain hidden and exposed station problem with suitable scenario.

Hidden Node Problem: Another major MAC layer problem specific to a WLAN is the hidden node issue, in which two stations on opposite sides of an AP can both hear activity from an AP, but not from each other, usually due to distance or an obstruction (see Figure 21.15a).

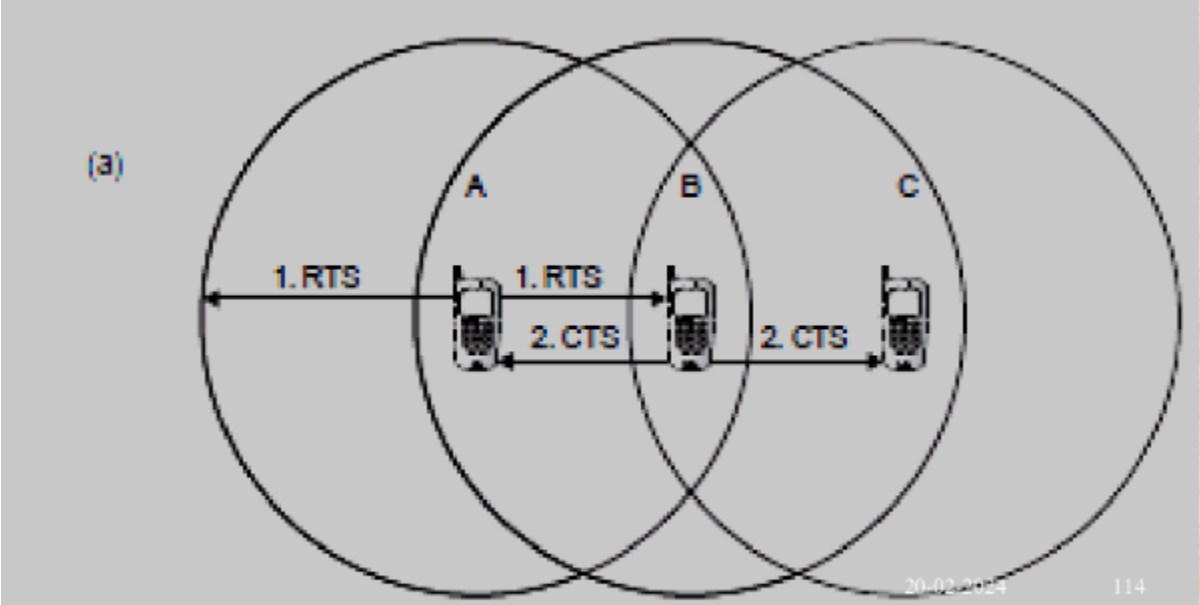


Figure 21.15(a) Hidden and exposed node problem.

- To solve this problem, 802.11 specifies an optional request to send/clear to send (RTS/CTS) protocol at the MAC layer.
- When this feature is in use, a sending station transmits an RTS and waits for the AP to reply with a CTS.
- Since all stations in the network can hear the AP, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision.
- Since RTS/CTS adds additional overhead to the network by temporarily reserving the medium, it is typically used only on the largest-sized packets, for which transmission would be expensive from a bandwidth standpoint.
- This mechanism reduces the probability of a collision on the receiver area by a station that is hidden from the transmitter to the short duration of the RTS transmission, because all stations hear the CTS and make the medium busy until the end of the transaction.
- The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledged
  station).
- It should also be noted that, due to the fact that RTS and CTS are short frames, the mechanism also reduces the overhead of collisions, since these frames are recognized faster than if the whole packet were to be transmitted.

- The mechanism is controlled by a parameter called RTS threshold, which, if used, must be set on both the AP and the client side.

Exposed node problem:

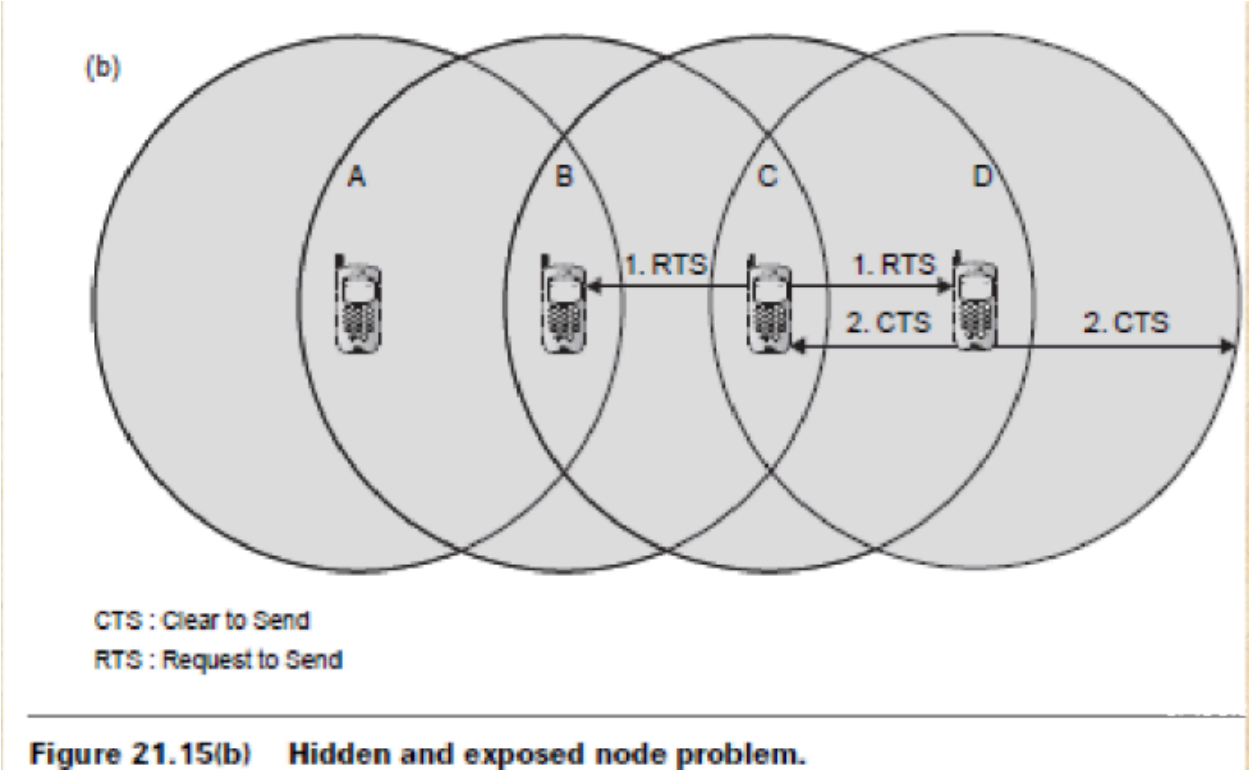


Figure 21.15(b) Hidden and exposed node problem.

- Assume that node B and C intend to transmit data only without receiving data. When node C is transmitting data to node D, node B is aware of the transmission.
- This is because node B is within the radio coverage of node C. Without exchanging RTS and CTS frames, node B will not initiate data transmission to node A because it will detect a busy medium.
- The transmission between node A and node B, therefore, is blocked even if both of them are idle.
- This is referred as the exposed node problem.
- To alleviate this problem, a node must wait a random backoff time between the two consecutive new packet transmission times.

10. Explain WEP frame security mechanism.

WEP (Wired Equivalent Privacy) frame security mechanism was one of the early encryption standards used in Wi-Fi networks. Here's an explanation of its functioning:

1. Initialization Vector (IV): WEP uses a 24-bit IV along with the secret key for encryption. IV is combined with the secret key to create the RC4 encryption key for each data packet.

2. RC4 Encryption: WEP uses the RC4 stream cipher for encryption. The RC4 key is generated by concatenating the secret key with the IV.

3. WEP Key: The WEP key is typically 40 or 104 bits in length, though 104-bit keys are more secure.

4. Shared Key Authentication: WEP uses a shared key authentication method where both the access point and the client share a common key. The client must prove it has the correct key by encrypting a challenge sent by the access point.

5. Open System Authentication: WEP also supports open system authentication where any client can authenticate itself to the access point, regardless of whether it possesses a valid key.

6. Weaknesses: WEP's security has been compromised due to several weaknesses, such as the small IV space, leading to IV reuse and statistical attacks, making it vulnerable to key recovery attacks.

7. Vulnerabilities: Attacks like the FMS attack and the KoreK Chopchop attack exploit weaknesses in WEP's design to recover the secret key.

8. Phasing Out: Due to its vulnerabilities, WEP has been largely phased out in favor of more secure encryption standards like WPA (Wi-Fi Protected Access) and WPA2.

11. What are main differences between Wimax and wifi.

PPT
802.16 = WiMax, 802.11 = WiFi
–
802.16e kya hai pata nai 👍

Parameters	*IEEE 802.16*	*IEEE 802.16a*	*IEEE 802.16e*
Spectrum	10–66 GHz	2–11 GHz	<6 GHz
Configuration	Line-of-sight	Non-line-of-sight	Non-line-of-sight
Bit rate	32–134 Mbps (28 MHz channel)	≤70 or 100 Mbps (20 MHz channel)	Up to 15 Mbps
Modulation	QPSK, 16-QAM, 64-QAM	256 subcarrier OFDM using QPSK, 16-QAM, 64-QAM, 256-QAM	Same as 802.16a
Mobility	Fixed	Fixed	≤75 Mph
Channel bandwidth	20, 25, 28 MHz	Selectable 1.25–20 MHz	5 MHz (planned)
Typical cell radius	1–3 miles	3–5 miles	1–3 miles

Parameter	*IEEE 802.11*	*IEEE 802.16*	*Explanation*
Range	30–100 m	Typical cell size: 7–10 km; up to 50 km; no hidden stations.	802.16 handles multipath propagation much better. Good signal quality in larger Distances
Target usage	Indoor	Outdoor; support of mesh topologies	802.16 is used outdoor.
Scalability	Bandwidth of 20 MHz is fixed	Bandwidth between 1.5 and 28 MHz allows an adaptation to the users.	802.16 has no problem with overlapping cells; usage of demand assignment multiple access (DAMA)–time division multiple access (TDMA) instead of CSMA/CA; adaptive modulation possible.

Parameter	*IEEE 802.11*	*IEEE 802.16*	*Explanation*
Data rate	Up to 54 Mbps	Up to 134 Mbps, depending on assigned bandwidth	OFDM with higher modulation ratio; net data rate also is higher (due to DAMA)
QoS	Only with 802.11e	Differentiated services	Reservation of capacity allows several service classes.
Costs	License-free	License-free as well as licensed bands.	Costs are accepted in 802.16 – alternative to xDSL

GPT

Applications	Suitable for providing broadband internet access over long distances	Ideal for local wireless connectivity such as internet access within homes, offices, and public hotspots
Standardization	Defined by IEEE 802.16 standards	Defined by IEEE 802.11 standards

12. Write short note on IEEE 802.16.

WiMAX: WiMAX is defined as worldwide interoperability for microwave access by the WiMAX Forum, promises to deliver last mile wireless broadband Internet access capable of carrying data intensive applications
-June 2001 to promote conformance and interoperability of the IEEE 802.16 standard, officially known as Wireless MAN.

- Some members of WiMAX(IEEE 802.16a) Forum are Airspan Networks, Alvarion, Aperto Networks, Ensemble Communication, Fujitsu of America, Intel, Nokia, Proxim, and Wi-LAN.

- The Forum describes WiMAX as "a standards-based technology enabling thedelivery of last mile wireless broadband access as an alternative to cable and digital subscriber line(DSL).

- WiMAX operates over licensed and non-licensed frequencies using non-line-of-sight (NLOS) and line-of-sight (LOS) technologies, extending broadband coverage to cities and towns wirelessly via a MAN.

- In NLOS, a small antenna on the mobile unit is connected to the WiMAX tower.

- In this mode, WiMAX uses a lower frequency range of 2–11 GHz (similar to Wi-Fi).

- In LOS, a fixed dish antenna points straight at the WiMAX tower from a rooftop or a pole.

- The LOS connection is stronger and more stable, so it is able to send a lot of data with fewer errors.

- LOS transmissions use higher frequencies, with ranges reaching approximately 66 GHz.

- the average cell ranges for most WiMAX networks have 4–5 mile range (in NLOS capable frequencies) even through tree cover and building walls.

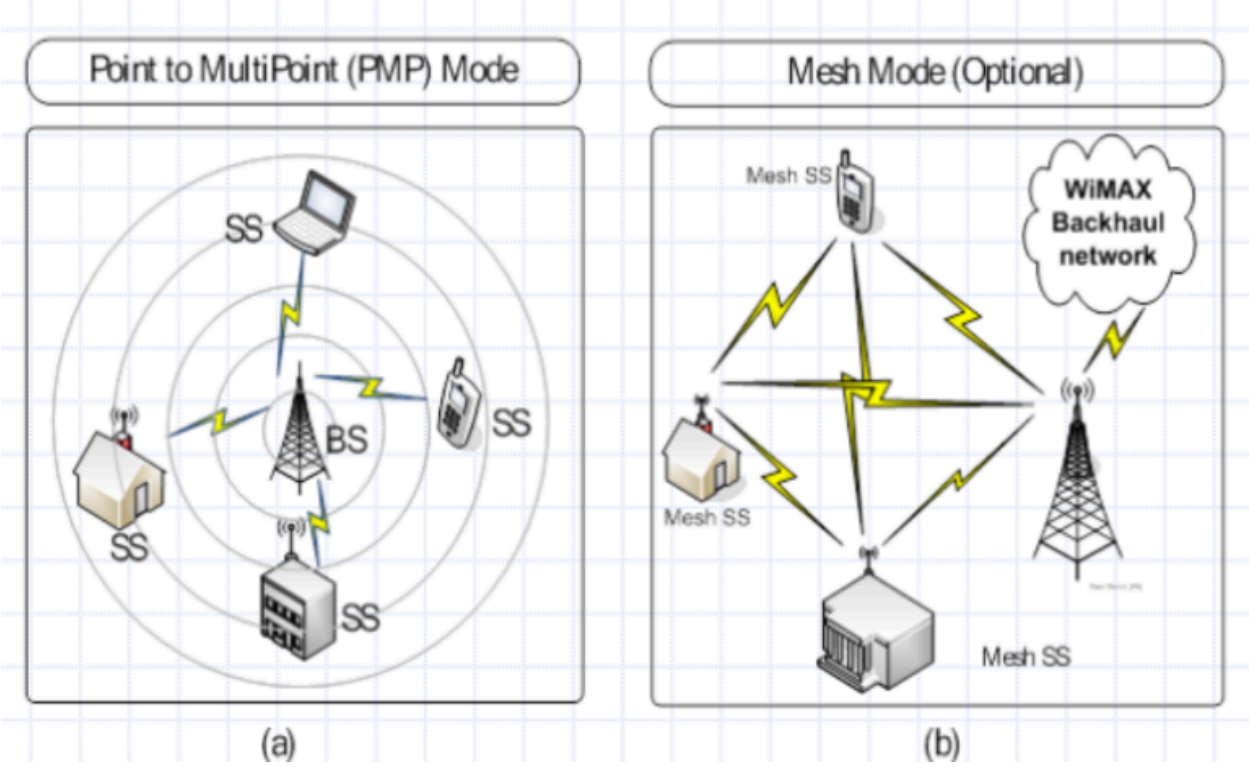
- Service ranges up to 10 miles (16 km) are very likely LOS applications.

- Ranges beyond 10 miles are possible but may not be desirable for heavily loaded networks.

13. Draw and explain IEEE 802.16 architecture.

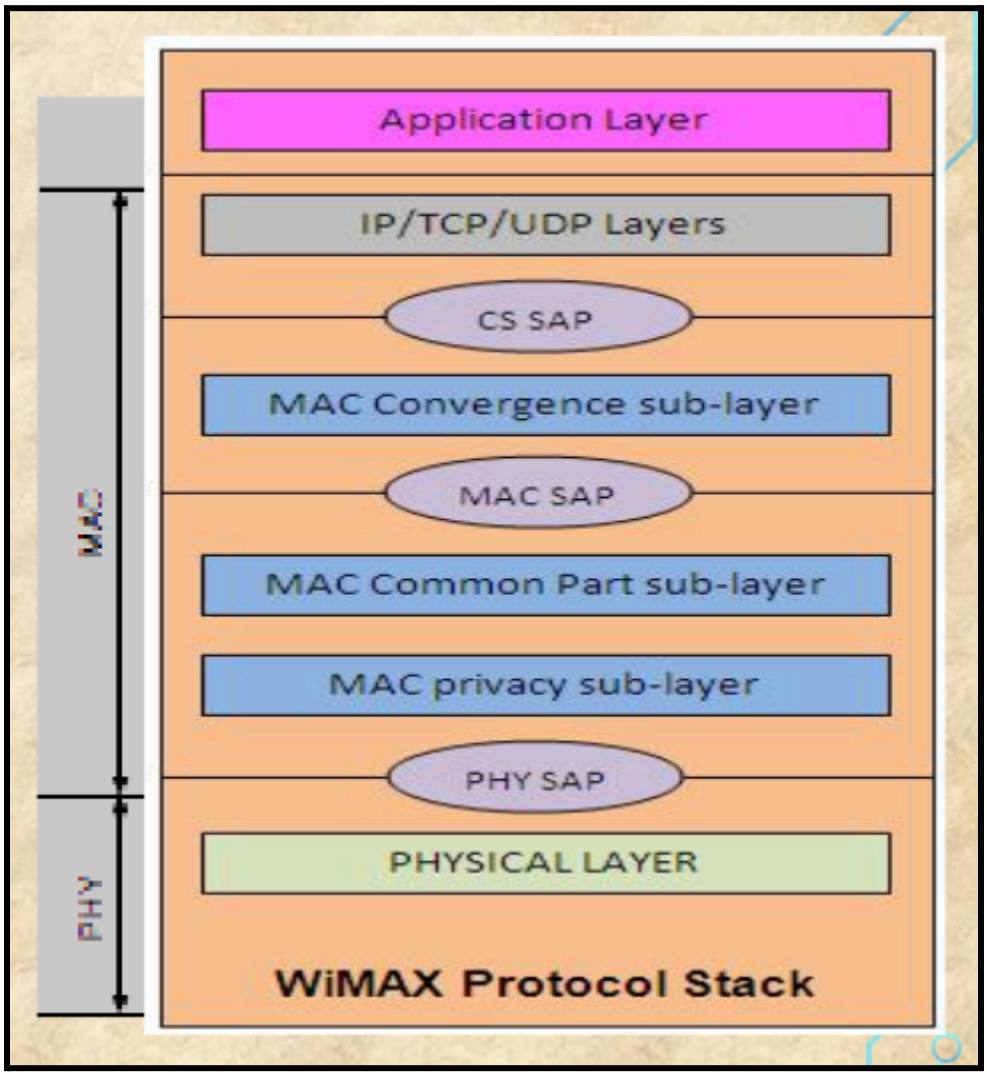
Architecture

- P2MP (Point to Multi point)
  - Wireless MAN
  - BS connected to Public Networks
  - BS serves Subscriber Stations (SS)
  - Provides SS with first mile access to Public Networks
- Mesh Architecture
  - Optional architecture for WiMAX



WT-module 3.pptx pg 16-24

14. Write short note on IEEE 802.16 protocol stack.



There are 2 layers:
1. MAC Layer
2. Physical Layer

1. The MAC layer is formed with three sublayers:

- **Service-specific convergence sublayer (CS),**
  The MAC CS receives higher level data through CS service access point (SAP) and provides transformation and mapping into MAC service data unit (SDU). MAC SDUs are then received by MAC CPS through MAC SAP.
  The specification targeted two types of traffic transported through IEEE 802.16 networks:
  1. Asynchronous transfer mode (ATM)
  2. Packets.

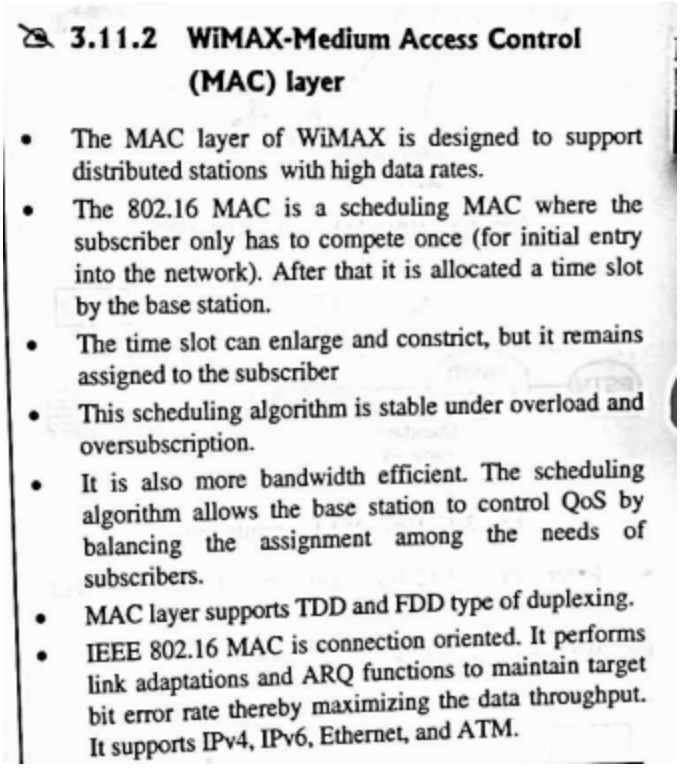
- **MAC common part sublayer (CPS),**
  It is core part of the MAC layer, defining medium access method.
  The CPS provides functions related to duplexing and channelization, channel access, packet data unit (PDU) framing, network entry, and initialization.
  This provides the rules and mechanism for system access, bandwidth allocation, and connection maintenance.
  QoS decisions for transmission scheduling are also performed within the MAC CPS.

- **Privacy sublayer.**
  The privacy layer lies between the MAC CPS and the PHY layer.
  Security is a major issue for public networks.
  This sublayer provides the mechanism for encryption and decryption of data transferring to and from PHY layer, and is also used for authentication and secure key exchange.
  Data, PHY control, and statistics are transferred between the MAC CPS and the PHY layer through the PHY SAP.

2. Physical Layer

The PHY layer includes multiple specifications which make the standard adaptable to different frequency ranges
Different variants of the IEEE 802.16 PHY layer with their capabilities and conditions of operation.
The original version of the standard on which WiMAX is based (IEEE 802.16) specified a PHY layer operating in the 10–66 GHz range.
802.16a, updated to 802.16-2004 in 2004, added specifications for the 2–11 GHz range.
802.16-2004 was updated by 802.16e-2005 in 2005 and uses scalable orthogonal frequency division multiple access (SOFDMA) as opposed to the orthogonal frequency division multiplexing version with 256 subcarriers.

15. Draw the frame format of Wimax MAC frame and explain various fields.



3.11.2 WiMAX-Medium Access Control (MAC) layer

- The MAC layer of WiMAX is designed to support distributed stations with high data rates.
- The 802.16 MAC is a scheduling MAC where the subscriber only has to compete once (for initial entry into the network). After that it is allocated a time slot by the base station.
- The time slot can enlarge and constrict, but it remains assigned to the subscriber
- This scheduling algorithm is stable under overload and oversubscription.
- It is also more bandwidth efficient. The scheduling algorithm allows the base station to control QoS by balancing the assignment among the needs of subscribers.
- MAC layer supports TDD and FDD type of duplexing.
- IEEE 802.16 MAC is connection oriented. It performs link adaptations and ARQ functions to maintain target bit error rate thereby maximizing the data throughput. It supports IPv4, IPv6, Ethernet, and ATM.

16. List the features of Wimax/ features of WiMAX(List features of IEEE802.16)

Flexible architecture:

- WiMAX supports several system architectures, including P2P, P2MP, and ubiquitous coverage.
- The WiMAX MAC supports P2MP and ubiquitous service by scheduling a time slot for each SS.
- If there is only one SS in the network, the WiMAX BS will communicate with the SS on a P2P basis.
- A BS in a P2P configuration may use a narrower beam antenna to cover longer distances

High security:

- WiMAX supports Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).
- By encrypting the links between the BS and the SS, WiMAX provides subscribers with privacy (against eavesdropping) and security across the broadband wireless interface.
- Security also provides operators with strong protection against theft of service.
- WiMAX also provides protection for data that are being transmitted by different users on the same BS.

WiMAX QoS:

- WiMAX can be dynamically optimized for the mix of traffic that is being carried.
- Five types of services are supported:
- unsolicited grant service (UGS),- fixed allocation is made by BS
- real-time polling service (rtPS),- BS regularly polls MS to findout allocation need. Hence bandwidth is allocated on need basis and is adaptive in nature
- extended real-time polling service (ertPS),- There will be no traffic transmission during silence time.
- non-real-time polling service (nrtPS),
- best effort (BE) service- BW is granted to mobile subscriber if and only there will be left over bandwidth from other QoS classes

Quick deployment:

- Compared with the deployment of wired solutions, WiMAX requires little or no external plant construction. Once the antenna and equipment are installed and powered, WiMAX is ready for service.

OFDM-based Physical Layer

- The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.

Very High Peak Data Rates

- WiMAX is capable of supporting very high peak data rates. In fact, the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum.
- More typically, using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

Support for Advanced Antenna Techniques

- The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing.

Flexible and Dynamic per User Resource Allocation

- Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

Mobility:

- The IEEE 802.16e amendment has added key features in support of mobility.
- The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.
- These improvements, which include scalable OFDMA,MIMO, and support for idle/sleep mode and handoff, will allow full mobility at speeds up to 160 km/h.

Cost-effective:

- WiMAX is based on an open, international standard. Mass adoption of the standard, and the use of low-cost mass-produced chipsets, will bring costs down

Wider coverage:

- WiMAX dynamically supports multiple modulation levels, including binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16 QAM, and 64 QAM.
- When equipped with a high-power amplifier and operating with a low-level modulation (BPSK or QPSK, for example), WiMAX systems are able to cover a large geographic area when the path between the BS and the SS is unobstructed.

NLOS operation:

- WiMAX is based on OFDM technology, which has the inherent capability of handling NLOS environments.
- This capability helps WiMAX products deliver broad bandwidth in an NLOS environment, which other wireless products cannot do.

High capacity:

- Using higher modulation (64 QAM) and channel bandwidth, WiMAX systems can provide significant bandwidth to end-users.