SECOND GENERATION (2G)

- 2G refers to the second generation of mobile networks.
- It is popularly based on GSM(Global System for Mobile communications) architecture.
- It uses digital signal. (circuit switching tech.)

Features of 2G network as improvement over 1G are:

- Data speeds of up to 64 kbps (1G = 2.4 kbps) (data in the form of sms)
- Use of digital signals(data and voice digitally encrypted: more security) instead of analog.
- digital signals consume less battery power compared to 1g
- Enabled services such as SMS and MMS
- Provided better quality voice calls (Reduced Noise as compared to 1G)
- It used a bandwidth of 30 to 200 KHz (Better Bandwidth Utilization)

Drawback

- It cannot handle complex data such as videos
- strong digital signal requirements

THIRD GENERATION (3G)

- 3G refers to the third generation of mobile networks.
- It is popularly based on UMTS(Universal Mobile Telecommunications System) architecture.
- 3G network upgrades 2G network with new technologies and protocols to deliver faster data rate. (packet switching technology)

Features of 3G network as improvement over 2G are:

- Data speeds 144 Kbps to 2 Mbps
- Send/receive large email messages
- Increased bandwidth : 15-20 MHz
- faster communication
- web based application can run(surfing webpages with audio and video) youtube with buffering, GPS etc

Drawback

- Expensive
- High Bandwidth requirement

FOURTH GENERATION (4G)

- 4G refers to the fourth generation of mobile networks
- The most important 4G standard :4G LTE
- 4G LTE is a “fourth generation long term evolution”, capable of delivering a very fast and secure internet connection by using IP protocols.
- The main difference between 3G and 4G is the data rate

Features of 4G network are:

- Data speeds of up to 100 Mbps to 1 Gbps
- Support interactive multimedia, voice, video.
- Increased bandwidth : 100 MHz
- supports HD mobile tv, video conferencing , and other services that requires high data speed

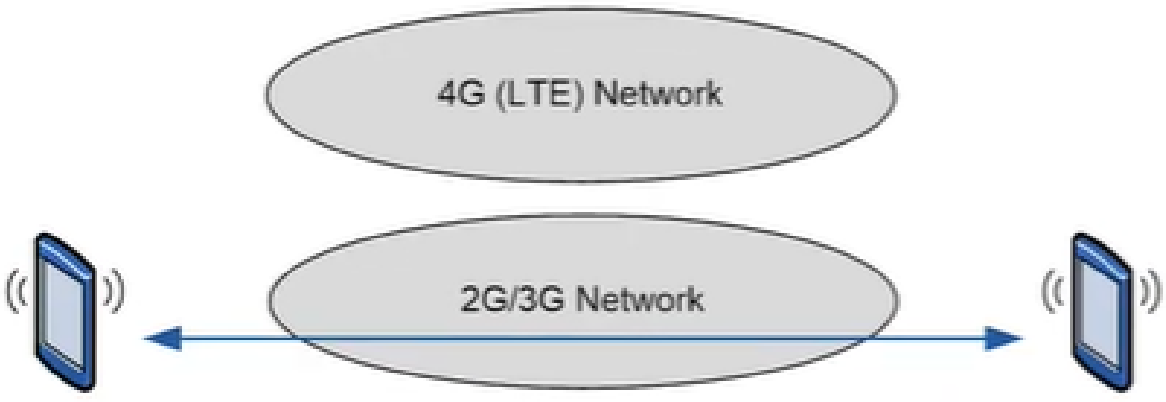
Drawback

- Expensive
- Complicated Hardware Requirements

- The only service 4G LTE provides Broadband data connection
- it doesn't support voice services.

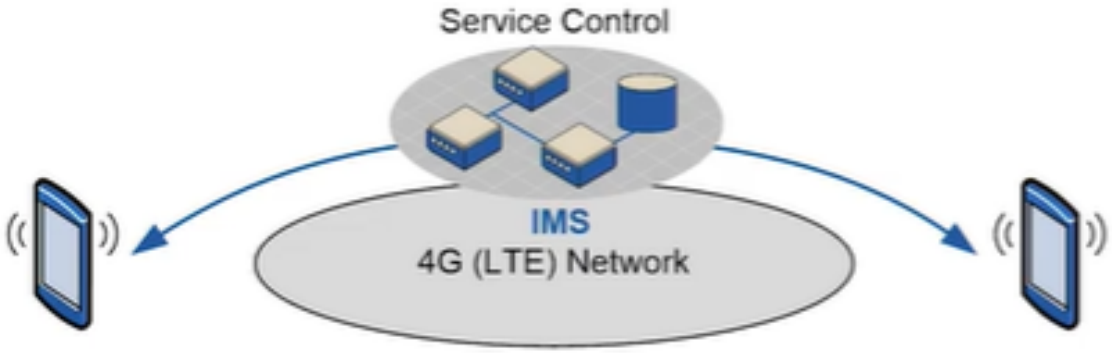
solution: 2 ways:

- 1. either pushing system to 2g/3g architecture



Without VoLTE, the mobile will have to disconnect from 4G and make a normal 2G/3G call (termed Circuit Switched Fallback)

or using VoLTE



The technology is termed “VoLTE” and requires a separate network called an IP Multimedia Subsystem to provide service control

Ad-hoc WLAN

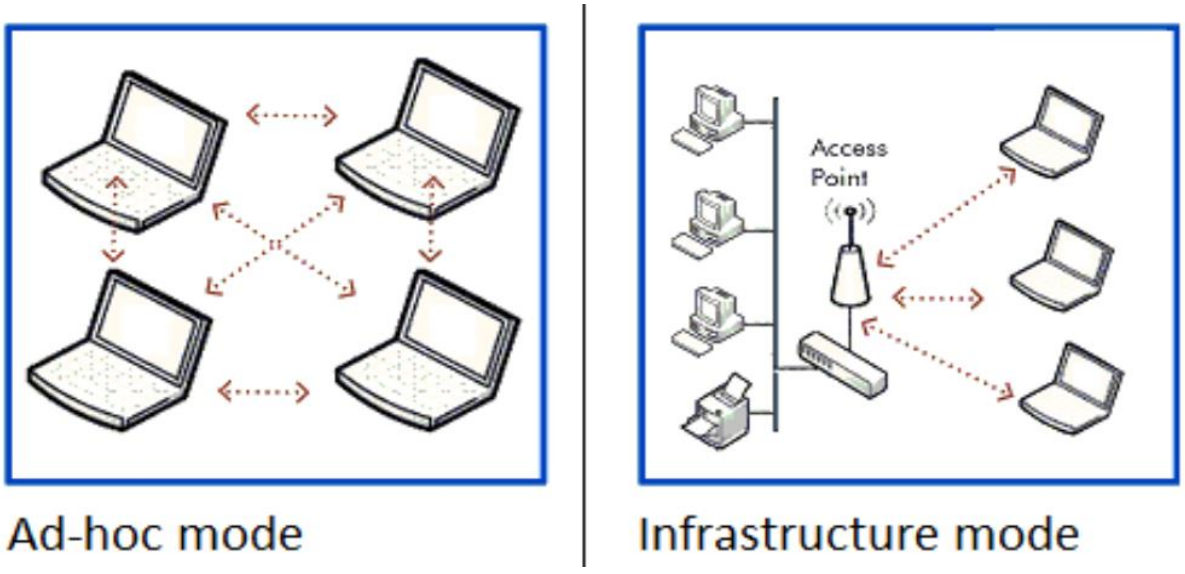
WLANs can be broadly classified into two types, infrastructure networks and ad hoc LANs, based on the underlying architecture.

Infrastructure networks

Infrastructure networks contain special nodes called access points (APs), which are connected via existing networks. APs are special in the sense that they can interact with wireless nodes as well as with the existing wired network. The other wireless nodes, also known as mobile stations (STAs), communicate via APs. The APs also act as bridges with other networks.

Ad hoc networks

Ad hoc LANs do not need any fixed infrastructure. These networks can be set up on the fly at any place. Nodes communicate directly with each other or forward messages through other nodes that are directly accessible.



How Ad-hoc network works?

Because the devices in the ad hoc network can access each other's resources directly through a basic peer-to-peer (P2P) wireless connection, central servers are unnecessary for functions such as file sharing or printing. In a WANET, a collection of devices, or nodes, is responsible for network operations, such as routing, security, addressing and key management.

Devices in the ad hoc network require a wireless network adapter or chip, and they need to be able to act as a wireless router when connected. When setting up a wireless ad hoc network, each wireless adapter must be configured for ad hoc mode instead of infrastructure mode. All wireless adapters need to use the same service set identifier (SSID) and wireless frequency channel number.

Instead of relying on a wireless base station to coordinate the flow of messages to each node in the network, the individual nodes in ad hoc networks forward packets to and from each other. Makeshift by nature, ad hoc wireless networks are useful where there is not a wireless structure built -- for example, if there aren't any access points or routers within range and cabling cannot be extended to reach the location where additional wireless communication is needed.

However, not all Wi-Fi networks are the same. In fact, Wi-Fi access points work in either ad hoc or infrastructure mode. Typically, Wi-Fi networks in infrastructure mode are created and managed using equipment such as Wi-Fi routers, wireless access points (WAPs) and wireless controllers. Ad hoc networks are also often short-lived networks created by a laptop or other device. The use of more sophisticated network protocols and network services found on infrastructure-based wireless networks usually are not suitable for ad hoc networks.

When should you use an ad hoc wireless network?

Deciding when to employ ad hoc versus infrastructure mode depends on the use. A user who wants a wireless router to act as a permanent access point should choose infrastructure mode. But ad hoc mode might be a good option for

a user setting up a temporary wireless network between a small number of devices.

Connecting devices to the internet using an ad hoc network.

Ad hoc networks are used frequently in new types of wireless engineering. They require minimal configuration and can be deployed quickly, which makes them suitable for emergencies, such as natural disasters or military conflicts. Thanks to the presence of dynamic and adaptive routing protocols, these networks can be configured quickly. These impromptu, on-demand networks are useful for putting together a small, inexpensive all-wireless LAN without the need for wireless infrastructure equipment. They also work well as a temporary fallback mechanism if equipment for an infrastructure mode network fails.

The following example shows one of the more popular uses for an ad hoc wireless network: connecting multiple wireless endpoints to the internet using an ad hoc intermediary device. Note that the intermediary device consists of a PC or laptop with a wired connection to the internet and a second wireless chip/antenna to connect other ad hoc wireless-capable devices to it for the purpose of sharing internet access.

Types of ad hoc wireless networks

Types of WANETs vary by application need and use. Choosing a wireless ad hoc network type depends on the wireless equipment capabilities, physical environment and purpose of the communication.

MANET. A mobile ad hoc network involves mobile devices communicating directly with one another. A MANET is a network of wireless mobile devices without an infrastructure that are self-organizing and self-configuring. A MANET is sometimes referred to as an "on-the-fly" or "spontaneous network."

IMANETs. Internet-based mobile ad hoc networks support internet protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol) and User Datagram Protocol (UDP). The iMANET employs a network-layer routing protocol on each connected device to link mobile nodes and set up distributed routes automatically. IMANETs may also be used in the collection of sensor data for data mining for a variety of use cases, such as air pollution monitoring.

SPANs. Smartphone ad hoc networks employ existing hardware, such as Wi-Fi and Bluetooth, and software protocols built into a smartphone operating system (OS) to create P2P networks without relying on cellular carrier networks, wireless access points or other traditional network infrastructure equipment. Different from traditional hub-and-spoke networks, such as Wi-Fi Direct, SPANs support multi-hop relays. Multi-hop relay is the process of sending traffic from device A to device C using intermediary device B. Therefore, device A and C do not need to have a direct P2P connection established for traffic to reach its destination. And because SPANs are fully dynamic in nature, there is no notion of a group leader in this type of application and, thus, peers can join or leave without harming the network.

Vehicular ad hoc network. This network type involves devices in vehicles that are used for communicating between them and roadside equipment. An example is the in-vehicle safety and security system, OnStar.

Advantages of a WANET

- Ad hoc mode can be easier to set up than infrastructure mode when just connecting two devices without requiring a centralized access point.

- Because ad hoc networks do not require infrastructure hardware such as access points or wireless routers, these networks provide a low-cost way of direct client-to-client communication.

- Ad hoc networks are easy to configure and offer an effective way to communicate with devices nearby when time is of the essence and running cabling is not feasible.

- Ad hoc networks are often secured to protect against attacks, as their temporary, often impromptu qualities can make them vulnerable to security threats.

Disadvantages of ad hoc networks

- One major drawback of wireless ad hoc networking is that some Wi-Fi-enabled technology, including certain Android devices, wireless printers and custom IoT sensors, don't support ad hoc mode because of its limitations and will only connect to networks in infrastructure mode by default. In some cases, third-party software can be installed on endpoint devices to enable ad hoc communications.

- Infrastructure mode is a better option than ad hoc mode for setting up a larger and more permanent network that can support far more endpoints.

- Ad hoc networks also do not scale well. As the number of devices in an ad hoc network increases, it becomes harder to manage because there is not a central device through which all traffic flows.

- Wireless ad hoc networks cannot bridge wired LANs or to the internet without installing a special-purpose network gateway.

- Devices in an ad hoc network cannot disable SSID broadcasting like devices in infrastructure mode can. As a result, attackers can find and connect to an ad hoc device if they are within signal range.

Usages of Ad-Hoc network

- **Military –**
  An ad hoc networking will give access to the army to maintain an network among all the soldiers, vehicles and headquarters.

- **Personal area network (PAN) –**
  It is a short range, local network where each nodes are usually related with a given range.

- **Crisis Condition –**
  Because it is fairly easy to create it can be used in time of crisis to send emergency signals.

- **Medical Application –**
  It can use to monitor patient.

- **Environmental Application –**
  It can be used to check weather condition, forest fire, tsunami etc.

Problems :

There are several problems that Ad Hoc network faces –

- Limited wireless range

- Packet losses

- Energy conservation because of limited batteries.

- Low-quality communications.

- Hidden-node problem creates collision if two device try to communicate with same receiver.

ALOHA

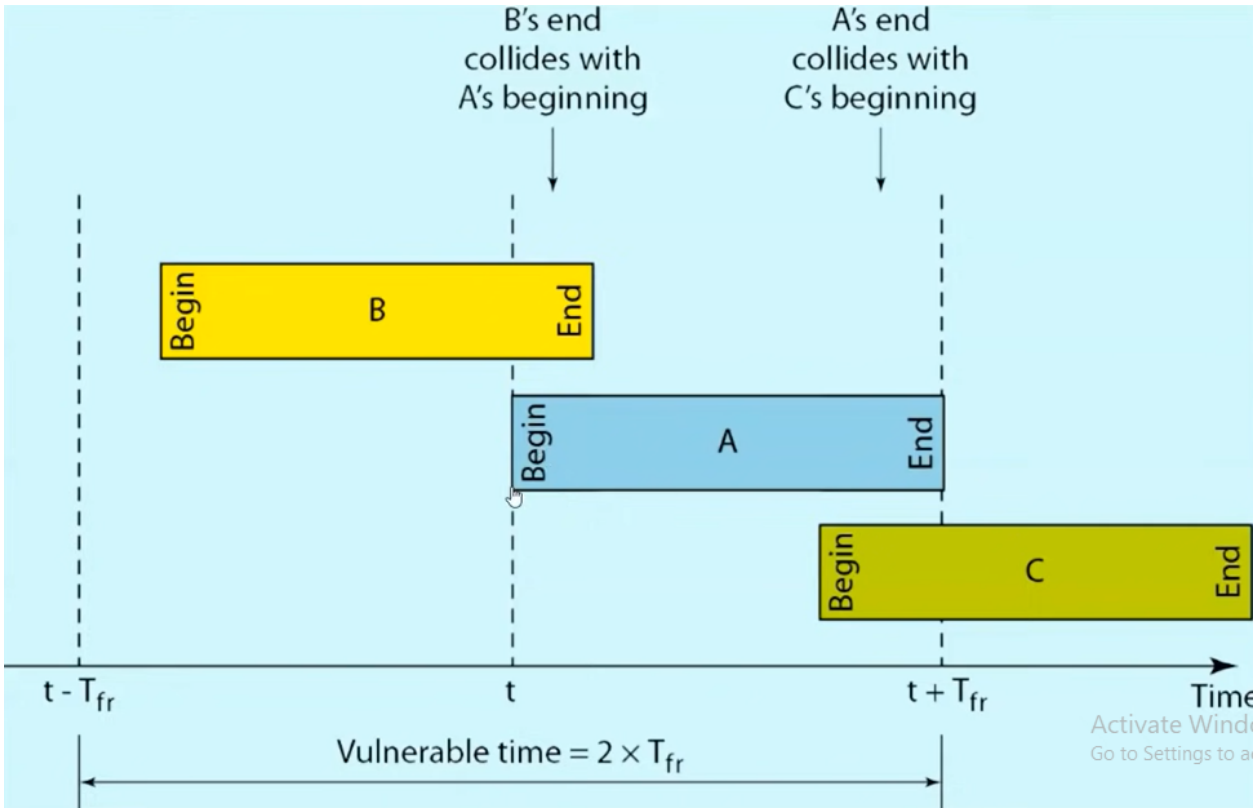
It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.
In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

Types:

Pure ALOHA

- Pure ALOHA allows stations to transmit whenever they have data to be sent.
- When a station sends data it waits for an acknowledgment.
- If the acknowledgment doesn't come within the allotted time then the stations wait for a random amount of time called Back-off time(Tb) and re-send the data.

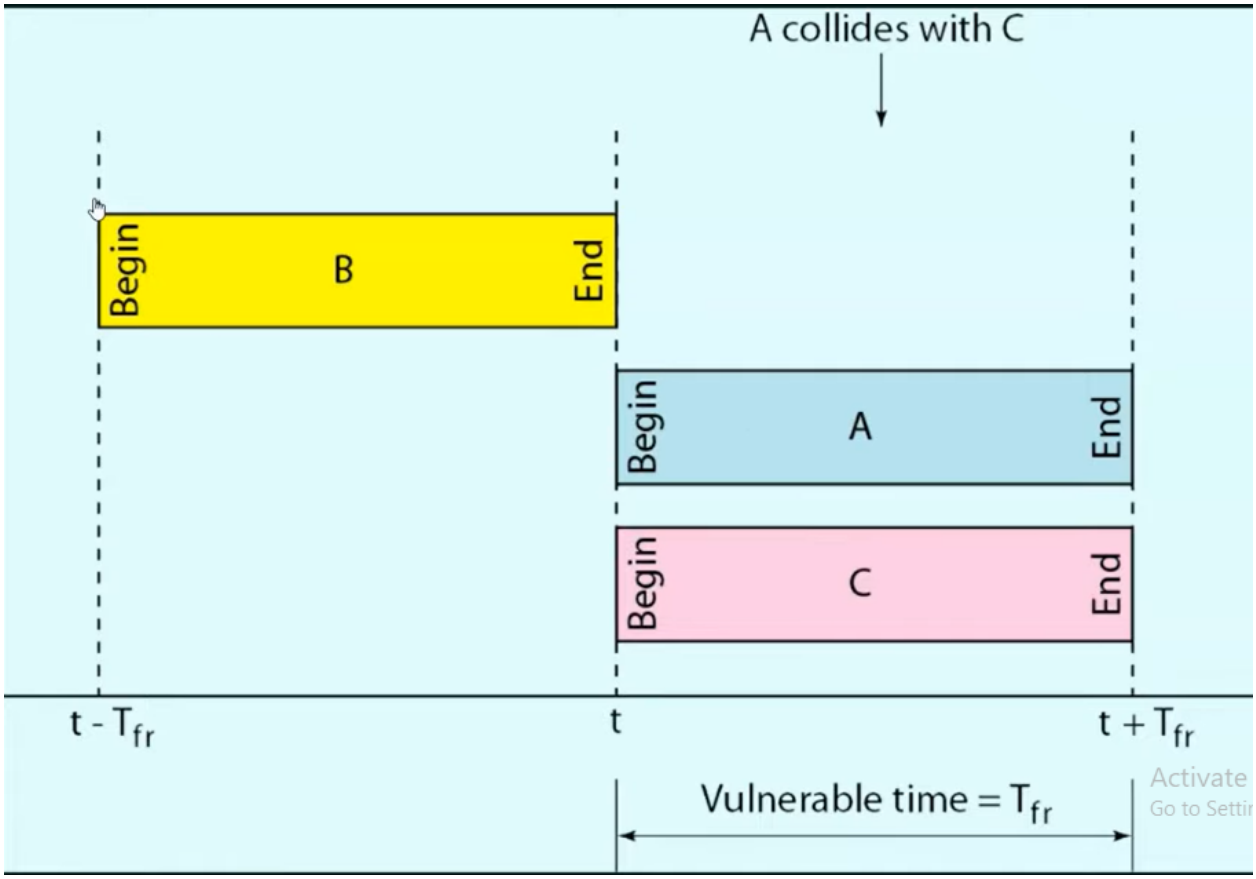
- Since different stations wait for a different amount of time, the probability of further collisions decreases.
- The Throughput of Pure ALOHA is maximized when frames are of uniform length.
- Whenever 2 frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
- If the first bit of the new frame overlaps with just the last bit of a frame almost finished both frames will be totally destroyed and both will have to be retransmitted later.



Vulnerable Time = $2*T_{fr}$
Throughput = $G*e^{-2G}$

Slotted ALOHA

- It was developed just to improve the efficiency of Pure ALOHA as the chances for collision in Pure ALOHA are high.
- The time of the shared channel is divided into discrete time intervals called slots.
- Sending of data is allowed only at the beginning of these slots.
- If a station misses out the allowed time, it must wait for the next slot.This reduces the probability of collision.



Vulnerable Time = Frame Transmission Time
Throughput = $G*e^{-G}$

Differences between Pure and Slotted ALOHA

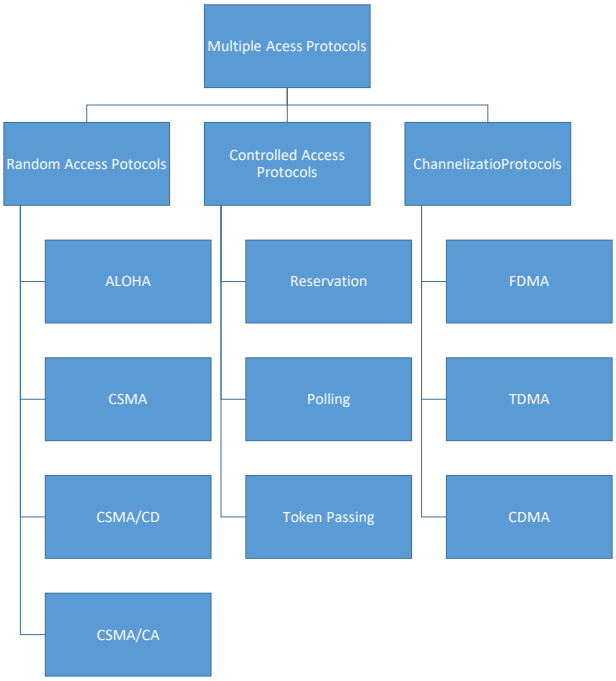
Pure Aloha	Slotted Aloha
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, Probability of successful transmission of the data packet = G x e-2Greduce	In Slotted Aloha, Probability of successful transmission of the data packet = G x e-G
Pure Aloha doesn't reduces the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%

CSMA/CA -NOTES

(Nitesh Kumar - 33, Tania Aggarwal - 60)

MULTIPLE ACCESS CONTROL

- If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there are no dedicated link present then multiple stations can access the channel simultaneously.
- Hence multiple access protocols are required to decrease collision and avoid crosstalk.
- **For example,** in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (**send data at same time**) then a lot of chaos is created (data overlap or data lost) then it is the job of the teacher (**multiple access protocols**) to manage the students and make them answer one at a time.
- Multiple access protocols can be subdivided further as –



Random Access

- In *random access* or *contention* methods, **no station is superior to another station** and
- none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to decide on whether to send.

- This decision depends on the state of the medium (**idle or busy**). In other words, each station can transmit when it desires on the condition that it follows the predefined procedure, including the testing of the state of the medium.

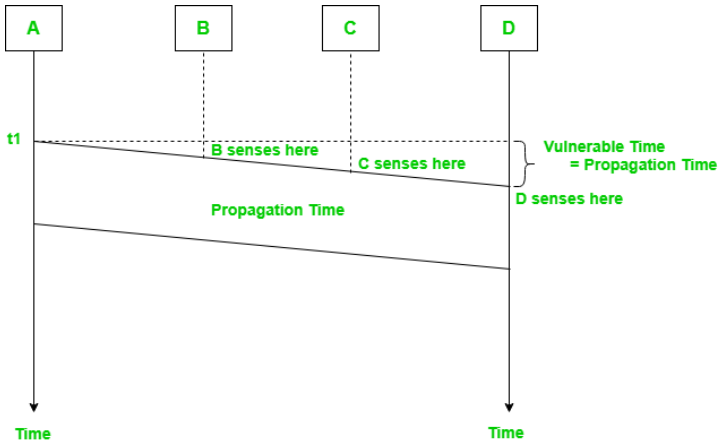
Two features give this method its name.

1. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access. Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.
2. In a random-access method, each station has the right to the medium without being controlled by any other station. However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified. To avoid access conflict or to resolve it when it happens, each station follows a procedure that answers the following **questions:**

- *When can the station access the medium?*
- *What can the station do if the medium is busy?*
- *How can the station determine the success or failure of the transmission?*
- *What can the station do if there is an access conflict?*

Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle "***sense before transmit***" or "***listen before talk***.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- Reason: -
- Stations are connected to a shared channel (usually a dedicated medium).
- The possibility of collision still exists because of ***propagation delay***.
- when a station sends a ***frame***, it still takes time (***although very short***) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.



1. At time tI' station B senses the medium and finds it idle, so it sends a frame.
2. At time t2 (t2> tI)' station C senses the medium and finds it idle because, currently, the first
3. bits from station B have not reached station C. Station C also sends a frame.
4. The two signals collide and both frames are destroyed

Vulnerable Time

- The vulnerable time for CSMA is the propagation time ***Tp***.
- This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a ***frame***, and any other station tries to send a frame during this time, a ***collision*** will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.
- The leftmost station ***A*** sends a frame at time ***tI'*** which reaches the rightmost station ***D*** at time ***tI + Tp***. The gray area shows the vulnerable area in time and space.

Persistence Methods

It is basically tells the station what to do when the channel is in different state .

1. What should a station do if the channel is busy?
2. What should a station do if the channel is idle?

Three methods have been devised to answer these questions:

1. I-persistent method
2. the nonpersistent method
3. the p-persistent method

I-Persistent

- The I-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with
- probability I).
- This method has the highest chance of ***collision*** because two or more stations may find
- the line idle and send their frames immediately.

Nonpersistent

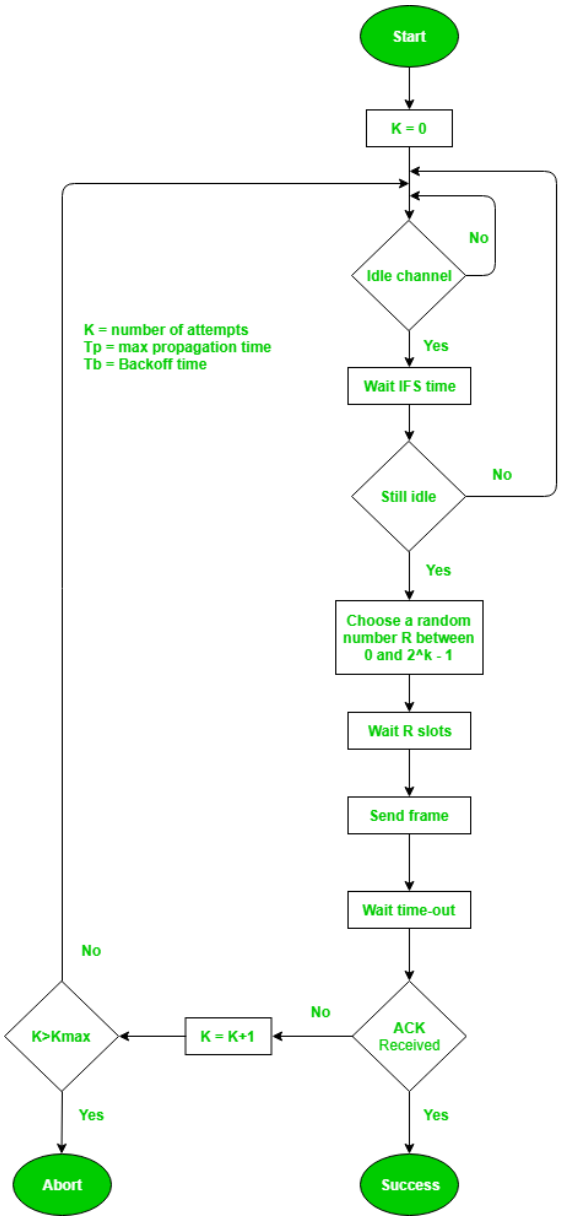
- In the nonpersistent method, a station that has a frame to send
- senses the line. If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.
- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-Persistent

- The p-persistent method is used if the channel has time slots with a slot
- duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.
- In this method, after the station finds the line idle it follows these steps:
    - With probability p, the station sends its frame.
    - With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
        - If the line is idle, it goes to step 1.
        - If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

CSMA/CA and Wireless Networks

CSMA/CA was mostly intended for use in wireless networks. The procedure described above, however, is not sophisticated enough to handle some issues related to wireless networks, such as hidden terminals or exposed terminals.



Steps:

1. First a station waits for IFS (inter frame space) that is decided by the network administrator.
2. To give priority to certain station like servers they can be assigned less IFS.
3. Every station then senses the carrier using methods (1-persistent, p-persistent, on-persistent).
4. As soon as the carrier is found **idle.** They do not immediately send they go and wait for Contention window depending on the attempt of the station.
   While waiting if the carrier gets busy in that case the station can wait here no need to go step 1.

5. After finishing the contention window waiting time station transmits the frame.
6. Now to ensure the delivery of the frame we use another mechanism that is Acknowledgement
7. This mechanism consists of time out time. If there is acknowledgement comes in the specified time, then the task is complete for that station
8. If there is no acknowledgement in the specified time, then the value of K becomes K+1
9. If the maximum number of attempts reached, then the operation is aborted.
10. If the attempt is within the limit (let say **Kmax**) then again, the whole process is repeated.

Distributed Coordination Function (DCF)

- Prabhu Tiwari 35

Two MAC sublayers: **the distributed coordination function (DCF)**

And **point coordination function (PCF)**

Distributed coordination function (DCF):

One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMAICA as the access method. Wireless LANs cannot implement CSMAfCD for **three reasons**:

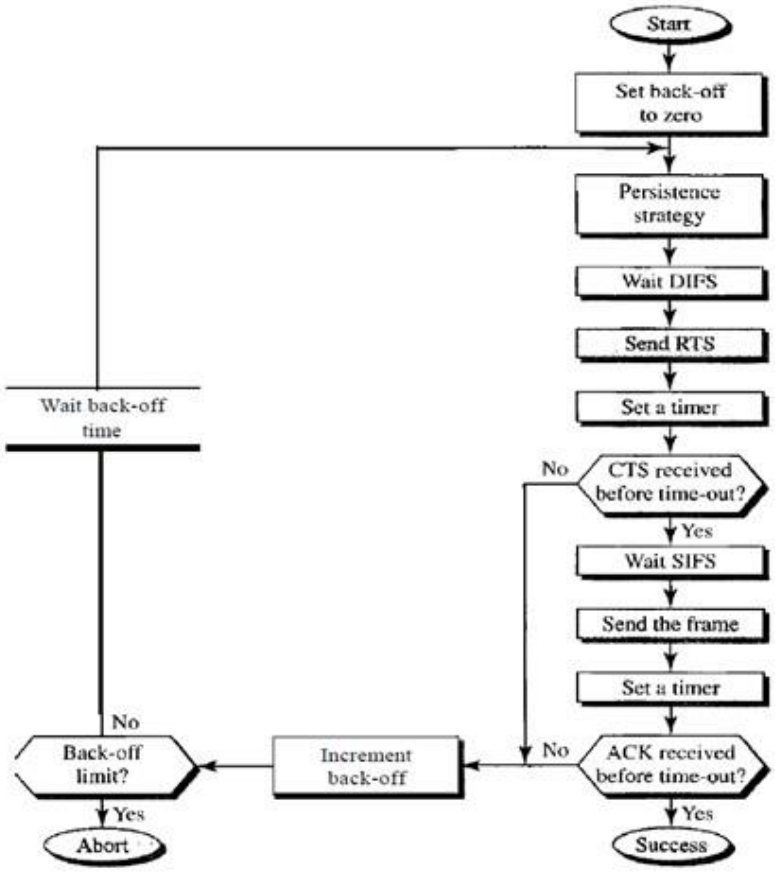
I. For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.

2. Collision may not be detected because of the hidden station problem.

3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Process Flowchart:

Figure 14.4 *CSMAICA flowchart*



I. Before sending a frame, the source station senses the medium by checking the
Energy level at the carrier frequency.

a. The channel uses a persistence strategy with back-off until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called
The distributed interframe space (DIFS); then the station sends a control frame called the request to send (RTS).
2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in *CSMAlCD* is a kind of indication to the source that data have arrived.

Network Allocation Vector How do other stations defer sending their data if one station acquires access? In other words, how is the *collision avoidance* aspect of this protocol accomplished? The key is a feature called NAV.

Direct Sequence Spread Spectrum (DSSS)

DSSS is the modulation method used for wireless LAN and ZigBee. DSSS transmissions multiply the data being transmitted by a “noise” signal. This noise signal is a pseudorandom sequence of 1 and -1 values, at a frequency much higher than that of the original signal. This noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence. This process is known as “de-spreading.”

Transmitter

The information signal undergoes primary modulation by phase shift keyed (PSK), frequency shift keyed (FSK), or other narrowband modulation and then secondary modulation with spread-spectrum modulation. Spread spectra are obtained by multiplying the primary modulated signal and the square wave, called the PN sequence. Alternatively, as in commercial radio, there are cases where spread modulation is applied to the data first, and narrowband modulation, such as PSK or FSK, is applied afterwards.

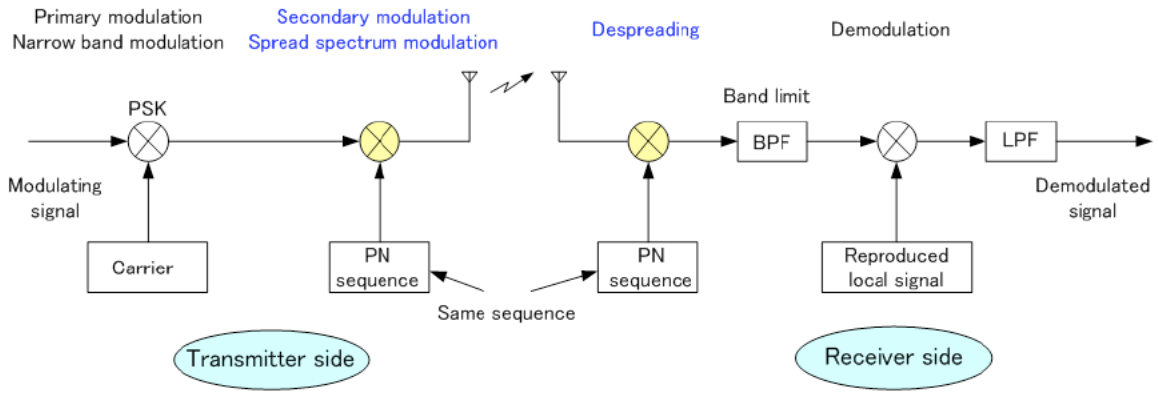


Figure 2: Spread spectrum modulation and demodulation using PSK for primary modulation.

Receiver

If despreading is applied to the received diffuse wave, it returns to the PSK or FSK modulated wave resulting from primary modulation. Then, as with narrowband demodulation, if the despread wave and local signal are multiplied, and appropriate low pass processing is applied, the information signal can be retrieved. Despreading involves multiplying the same PN code as that used at the transmitting end for the receiving wave. It is necessary to synchronize the receiving wave and PN code.

There are two processing methods on the receiving side, demodulation of the information signal after despreading, and obtaining a positive and negative PN code by multiplying the local signal by the receiving wave and despreading using correlation detection. With the former there is process gain but the problem of synchronization

remains. With the latter, the spectrum density of the receiving wave itself is low, and regeneration of the local carrier for performing synchronous detection is a problem. Commercial SS radio equipment uses the latter, but it requires considerable power and has a short communication range.

Despreading

The signal that enters the antenna of the receiver includes outside interference waves and noise. If this signal is despread, the signal component returns to a narrowband modulated wave and the interference components are diffused, expanding the spectrum infinitely so that its power density falls. Therefore, by inputting the signal with frequency band restricted using a band-pass filter, the interference component power that falls into the demodulation frequency band is reduced. The occurrence of errors is calculated using a stochastic process, so ultimately, using spread spectrum results in fewer errors, and thus spread-spectrum communication is resistant to interference.

Demodulation

Demodulation is normal narrowband demodulation. The local signal is regenerated from the receiving wave and after multiplication by the receiving wave, unnecessary components are eliminated with a low-pass filter. Primary modulation uses PSK, so synchronous detection is necessary.

PN sequence

The PN sequence is switched at a far faster speed than the symbol rate of the information signal and its spectrum covers a wide band. For this reason, the spectrum of the modulated wave after primary modulation also covers a wide band.

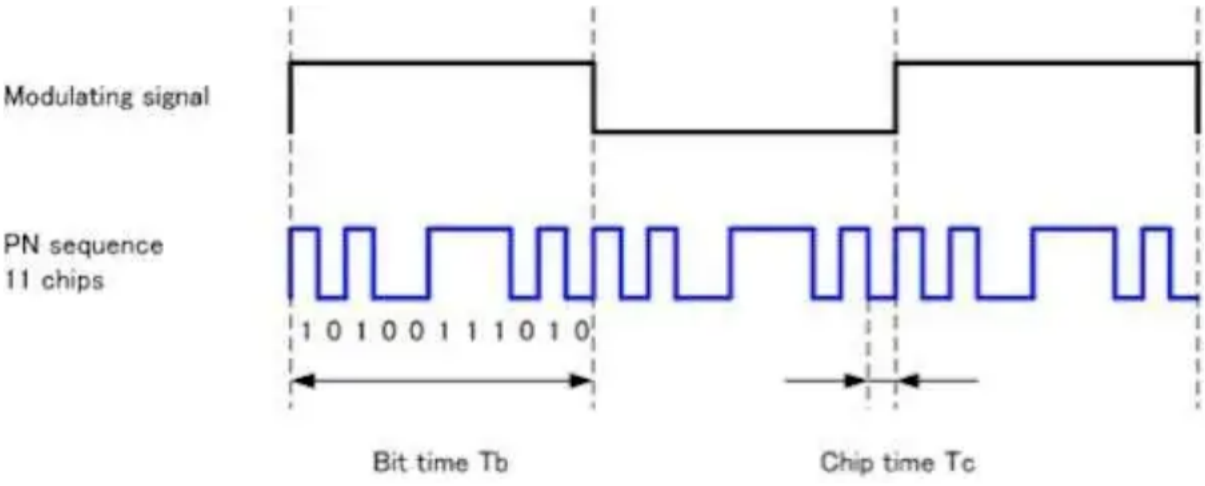


Figure 3: PN sequence

Advantages of DS-SS System

1. This system is the most effective at detecting and preventing deliberate interference (jamming).

2. For multipath signals, this system has a very high level of discrimination. As a result, the multipath interference is successfully reduced.

3. When compared to other systems, the DS-SS system outperforms them in the presence of noise.

Disadvantages of DS-SS system

1. The output rate of the PN code generator must be high. The length of such a series must be sufficient to ensure that it is genuinely random.

2. The acquisition time using the serial search method is too long. As a result, the DS-SS system is sluggish.

3. The varying distance between the transmitter and receiver affects synchronization.

4. The DS-SS signal is ineffective in the case of broadband interference.

Applications of DS-SS system

1. Anti-jamming application — protecting a jamming signal.

2. Signal transmission with low detectability - the signal is intentionally delivered at a very low power level. As a result, the signal is known as an LPI signal since it has a low probability of being intercepted (LPI).

3. Supporting numerous simultaneous signal transmissions on the same channel, such as with Code Division Multiple Access (CDMA) or spread spectrum multiple access (SSMA).

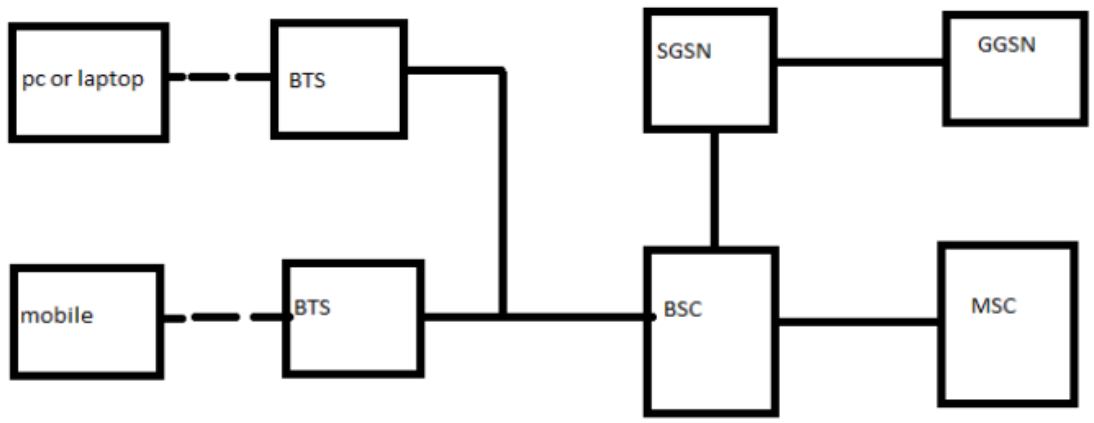
Enhanced Data Rate for GSM Evolution

EDGE (Enhanced Data Rate For GSM Evolution) provides a higher rate of data transmission than normal GSM. It uses a backward-compatible extension of GSM of digital mobile technology. EDGE has a pre-3G radio technology and uses part of ITU's 3G definition. It can work on any network deployed with GPRS (with necessary upgrades).

In order to increase data transmission speed, EDGE was deployed on the GSM network in 2003 by Cingular in the USA.

Working

It uses 8PSK modulation in order to achieve a higher data transmission rate. The modulation format is changed to 8PSK from GMSK. This provides an advantage as it is able to convey 3 bits per symbol, and increases the maximum data rate. However, this upgrade required a change in the base station.



EDGE In GSM Network

Features

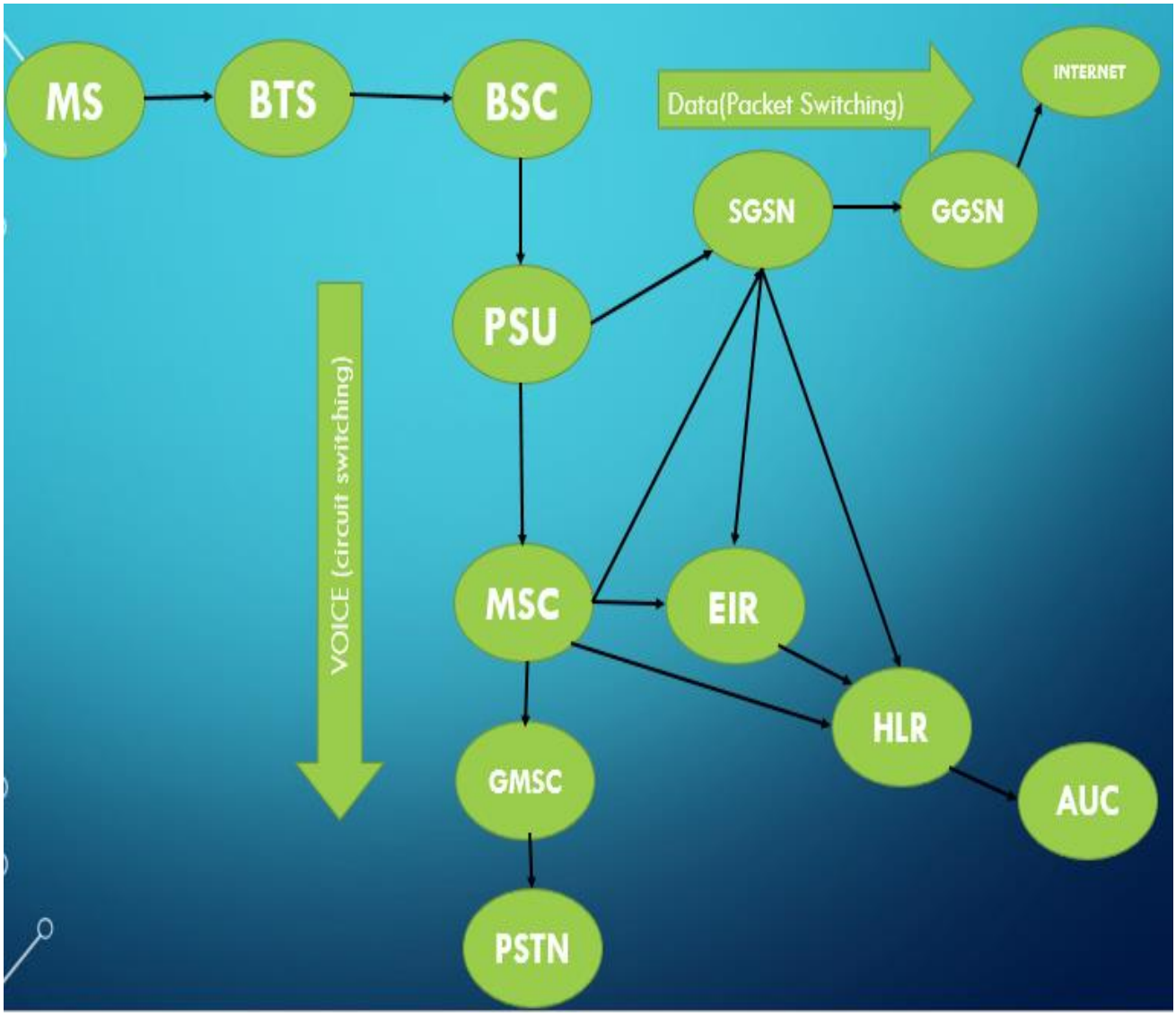
- It provides an evolutionary migration path from GPRS to UMTS.
- It is standardized by 3GPP.
- EDGE is used for any packet switched application, like an Internet connection.
- EDGE delivers higher bit-rates per radio channel and it increase the capacity and performance.

Advantage

- It has higher speed.
- It is an “always-on” connection
- It is more reliable and efficient
- It is cost efficient

Disadvantage

- It consumes more battery.
- Hardware needs upgradation.



FDD

Frequency division duplex (FDD) is a communication technique where the connected parties can communicate with each other in both directions through use of separate frequency bands for transmitting and receiving. Since FDD uses different frequency bands for upstream data and downstream data, the sending and the receiving signals do not interfere with each other.

FDD in Cellular Networks

Cellular networks use FDD to separate the channels. One block of the electromagnetic spectrum is allocated for uplink, which carries data from mobile phones to a base station. A different block of the spectrum is allocated to downlink, carrying data from a base station to mobile phones. Each of the blocks are divided into a number of channels.
In advanced mobile phone systems (AMPS), 832 full-duplex channels are used, each comprising of a pair of simplex channels, one for uplink and the other for downlink. The uplink channels are separated from the downlink channels through guard bands.

Advantages

➨It uses paired spectrum on continuous basis for both the directions and hence it can achieve higher rates for similar distances as TDD system.
➨Due to above, FDD system requires fewer base stations (or eNBs) compare to TDD as it covers larger distances with same rates as of TDD.
➨Due to requirements of less number of Base Stations, overall deployment, operation and maintenance costs are less

Disadvantages

➨In FDD, frequencies are allocated dedicately. This leads to wastage of spectrum when it is not used. Moreover guard band is used between uplink and downlink to avoid interference, this part is wasted as it is not used for useful traffic.
➨ FDD can not be deployed where spectrum is un-paired.
➨Though it saves in number of Base Station requirements, hardware costs associated with FDD are higher

Frequency Hopping Spread Spectrum

Spread Spectrum

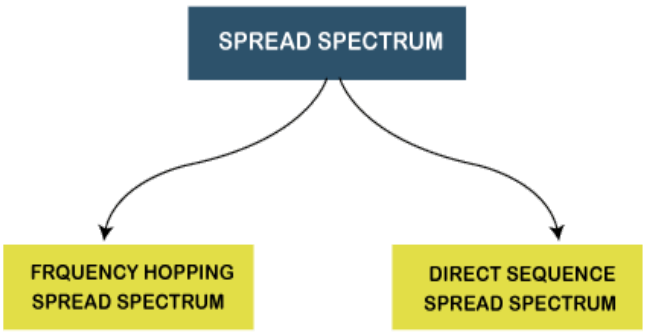
Spread Spectrum is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth.

Spread spectrum technology is widely used in radio signals transmission because it can easily reduce noise and other signal issues.

Types of Spread Spectrum

Spread Spectrum can be categorised into two types:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum(DSSS)



What is FHSS ?

- Frequency-hopping spread spectrum is designed for robust operation in noisy environments by transmitting short packets at different frequencies across wide portions of channel bandwidth.
- In many wireless networks, we use the frequency hopping spread spectrum for the purpose of improving communication quality and reliability. By using FHSS, it is possible to make communication more resistant to interference-causing noise.

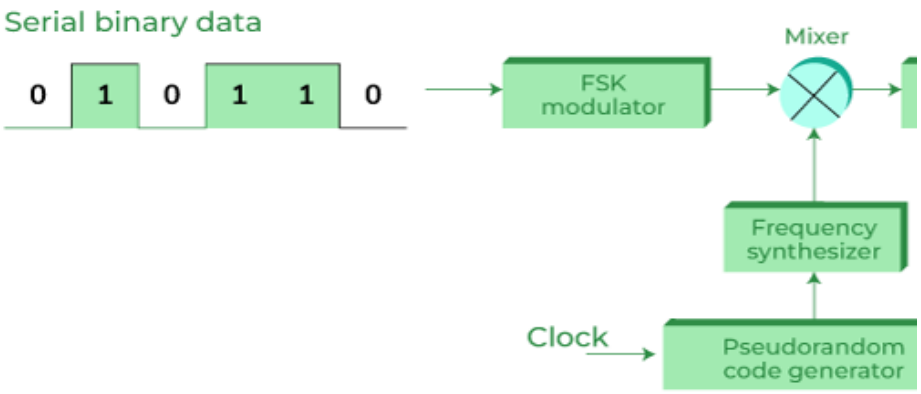
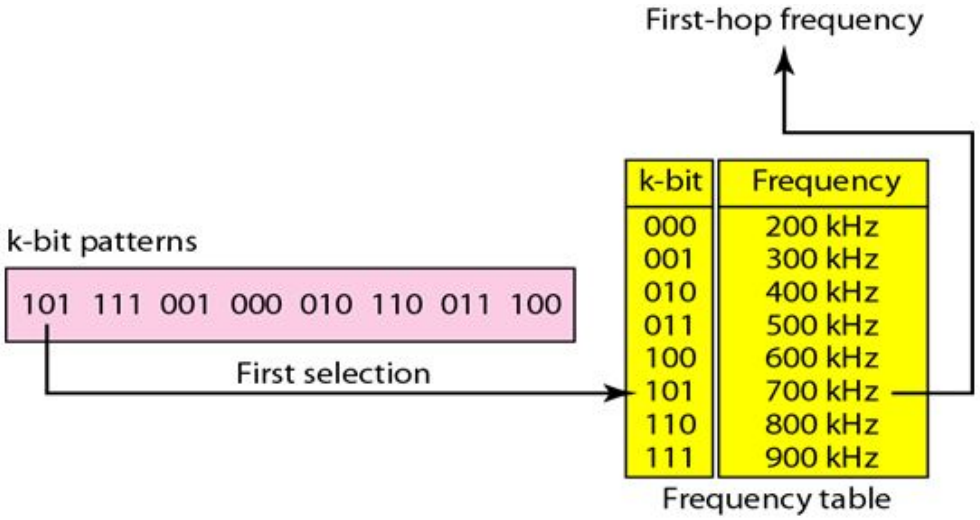


Fig. Block diagram of FHSS

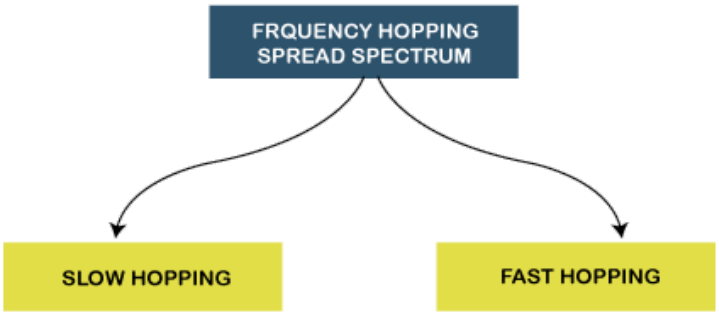


How does it work ?

- For transmission, binary data is fed into a modulator using some digital-to-analog encoding scheme, such as *Frequency Shift Keying (FSK) or Binary Phase Shift Keying (BPSK)*.
- A PN source serves as an index into a table of frequencies each K bit on the PN source specifies one of the 2k carrier frequencies.
- At each successive interval, a new carrier frequency is selected.
- This frequency is then modulated by the signal produced from the initial modulator to produce a new signal with the same shape.

- On reception, the spread spectrum signal is demodulated using the same sequence of PN-derived frequencies and then demodulated to produce the output data.

Types of FHSS



Sr.No.	Slow Frequency Hopping (SFH)	Fast Frequency Hopping (FFH)
1	As the name suggests, frequency hopping takes place slowly.	As the name suggests, frequency hopping takes place at a fast rate.
2	In this case, one or more data bits are transmitted within one frequency hop.	In this case one data bit is divided over multiple frequency hops.
3	One or more data bits are transmitted over the same carrier frequency.	One data bit is transmitted over multiple carriers in different frequency hops.
4	A jammer can detect this signal if carrier frequency in one hop is known.	A jammer can't detect this signal because one symbol is transmitted using more than one carrier frequency.
5	It supports coherent data detection.	It does not support coherent signal detection. It is very difficult in FFH.

Advantages of FHSS

The following are some advantages of frequency hopping spread spectrum (FHSS):

- High efficiency.

- Highly resistant to narrowband interference
- Requires a shorter time for acquisition.
- Highly secure. Its signals are very difficult to intercept if the frequency-hopping pattern is not known.
- Provides a very large bandwidth.

Disadvantages of FHSS

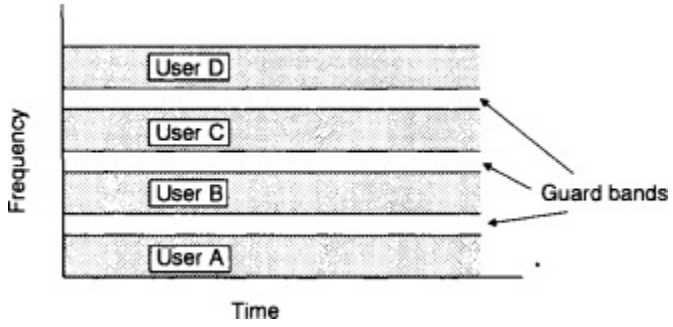
- Less Robust, so sometimes it requires error correction.
- Needs complex frequency synthesisers.
- Supports a lower data rate of 3 Mbps as compared to the 11 Mbps data rate supported by DSSS.

Applications of FHSS

- Used in wireless local area networks (WLAN) standard for Wi-Fi.
- Used in the wireless personal area networks (WPAN) standard for Bluetooth.

Frequency division multiple access

Principle : FDMA works on the principle of dividing the total bandwidth of the communication channel into a number of discrete segments and allocating each segment exclusively to a user.



FDMA is the most basic way of creating channels, by assigning users to non overlapping frequency bands, it was used in first and 2G cellular systems.. In a system with N users and a total bandwidth W, each user can be assigned a bandwidth of W/N.

Guard bands are used between each segment of the frequency band to prevent interference between users.

Number of Channels in FDMA

Let B_{total} be the total system bandwidth, B_{guard} be the guard band at edge and B_{ch} the single radio channel bandwidth. Then the number of channels in FDMA system :

$$N = B_{total} - 2B_{guard} / B_{ch}$$

The **advantage** of the FDMA system is its simplicity since once the channel capacity is divided amongst users each can operate independently of the other. Since each user has exclusive use of its allocated bandwidth there is no contention and therefore no wastage of bandwidth or delays caused by collisions and retransmissions.

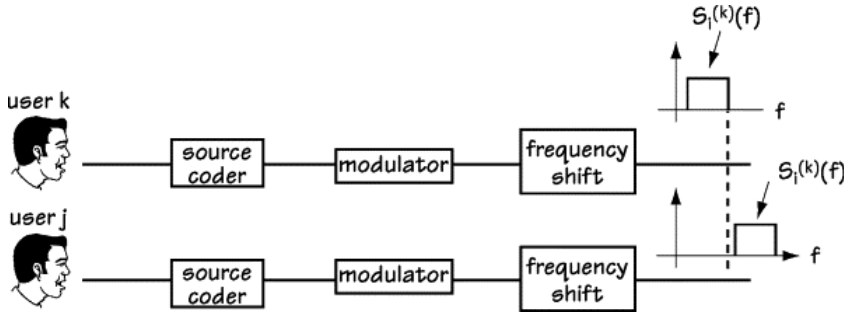
The **disadvantage** of FDMA systems is that there is a wastage of bandwidth, firstly caused by the guard bands and secondly due to the fact that users can only use their own allocated frequency bands. Therefore if a user needs more

information to transmit its given band lies idle, even though other users may have a considerable amount of information to send and are experiencing delays on their channel. FDMA is therefore best for use in systems where all users have a stream of data to send, and it is unsuitable for users with ‘bursty’ traffic, where contention systems, such as ALOHA, perform better.

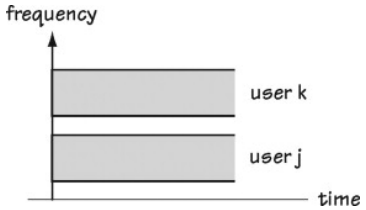
Another **disadvantage** of fixed assignment systems, such as FDMA, is that the number of users cannot easily be changed. This would require the overall channel frequency band to be redivided amongst the new users.

FDMA is also not suitable for use in systems that require the broadcast of data to many users. Since each user is allocated a single frequency band, it sends on this band and the receiver also monitors it.

An example of FDMA :
There, we see user k sending his information at one frequency and user j sending her information at a different frequency. If you know who you want to listen to, you tune your receiver to pick up transmissions at the desired user’s frequency. This system satisfies Equation , because user k is 0 at the frequencies where user j is transmitting, and user j is 0 at frequencies where user k is transmitting. That makes $s_i^k(f)s_i^j(f) = 0$, therefore $s_i^k(f)s_i^j(f)df = 0$.



The use of FDMA is also shown in Fig. Here, we see that each user is given all the time they could ever want, but they can only communicate over a small frequency band.



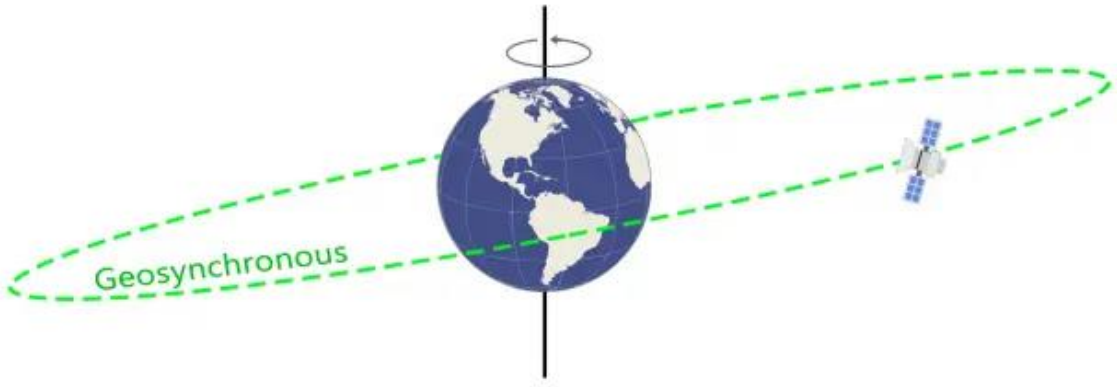
Geosynchronous Satellite

Overview

Geosynchronous satellites are satellites in a geosynchronous orbit—a geocentric orbit that has the same orbital period as the rotational period of the Earth. The orbit has a semi-major axis of 42,164 kilometers or 26,200 miles. In a more general case, when the orbit has some inclination or eccentricity, the satellite appears to describe a more or less distorted figure-eight in the sky, and essentially rests above the same spot of the Earth's surface once per sidereal day.

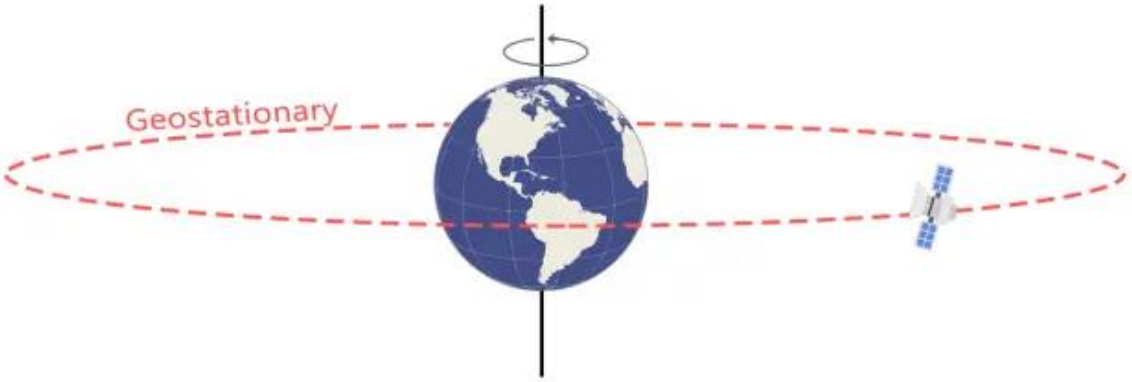
Geosynchronous and geostationary orbits

The geosynchronous orbit is also sometimes described as a geostationary orbit. Although there is some difference between the two orbits, they are also related. Both orbits are about 35,786 kilometers above Earth's surface, which puts it in a high Earth orbit category. At any inclination, a geosynchronous orbit synchronizes with the rotation of the Earth.



An example of a geosynchronous orbit.

While a geosynchronous orbit can have any inclination, geostationary orbits lie on the same plane as the equator; this is the key difference between these two types of orbits.



An example of a geostationary orbit, a sub-category of geosynchronous orbits.

Weather monitoring satellites like GOES are in geostationary orbits because they have a constant view of the same area. In a high Earth orbit, these satellites can also be useful for search and rescue beacons.

Advantages of GEO or Geosynchronous Earth Orbit

Following are the **advantages of GEO orbit**:

➡As it is at greater height, it covers larger geographical area. Hence only 3 satellites are required to cover the entire Earth.

➡Satellites are visible for 24 hours continuously from single fixed location on the Earth.

➡It is ideal for broadcasting and multi-point distribution applications.

➡Ground station tracking is not required as it is continuously visible from earth all the time from fixed location.

➡Inter-satellite handoff is not needed.

➡Less number of satellites are needed to cover the entire earth. Total three satellites are sufficient for the job.

➡Almost there is no doppler shift and hence less complex receivers can be used for the satellite communication.

Disadvantages of GEO or Geostationary Earth Orbit

Following are the **disadvantages of GEO orbit**:

➡The signal requires considerable time to travel from Earth to satellite and vice versa. The signal travel delay is about 120ms in one direction. The distance of 35786 Km gives 120 ms latency with $3x10^8$ m/sec speed of the signal. Hence it is

not suitable for point to point applications requiring time critical applications such as real time voice, video etc.

➡Since GEO orbit is located above the equator, it is difficult to broadcast near the polar region.

➡Due to longer transmission distance, the received signal is very weak. This requires better LNA (Low Noise Amplifier) and also advanced signal processing algorithms in the satellite modem. This increases cost of the ground station equipments.

➡It provides poor coverage at higher latitude places usually greater than 77 degrees.

GEO satellite maintenance

Due to the increased collision risk, and the relative importance of these satellites for communication and navigation systems, geosynchronous orbit maintenance has become an increasingly important issue. These satellites maneuver frequently and require the ability to detect unknown maneuvers for target satellites and to allow those satellites to recover an accurate orbit. Studies have been used to determine if angles from ground-based optical tracking to detect maneuvers and recover orbits can be used. One such tool, developed by Analytical Graphics Inc, uses sequential estimation software that uses a parametric study of maneuver size and time required to detect a maneuver. The company has also suggested various methods to recover the orbit after such maneuvers have been detected. This work is important towards developing more automatic methods of detecting maneuvers for a large population of active geosynchronous satellites.

Use cases for geosynchronous orbits

Due to the near stationary position of geostationary satellites, they have been used for global communications, television broadcasting, weather forecasting, and defense and intelligence applications.

Communications

For communications, a large geostationary satellite can provide a large amount of capacity across up to a third of the Earth's surface, and a network can cover the Earth with only three satellites. Further, these satellites can use multiple bands to allow a single satellite to layer capacities.

Government communications

For government communications, this can ensure that a network is capable of delivering greater capacity as required and that governments can achieve availability and reliability when moving to a new situation or location at short notice. However, one complication with newer communication systems and GEO satellites is the latency introduced through the distance of the orbit from the terrestrial stations. With GEO satellites, there can be latency up to 0.25 seconds between signal origination and reception. In part, this has driven the popularity of low Earth orbit satellites for emerging communications systems for their lack of latency.

Internet-based communications

However, with low Earth orbit satellites, a signal has to be swapped every seven minutes, and this switching is considered a possible point of failure or interruption with a signal, while a GEO satellite remains "fixed" and does not suffer from this possible point of friction.

Telecommunications

Geosynchronous satellites have long been a major medium for linking together terrestrial telecommunications networks. Satellite systems share the frequency spectrum with other satellite systems, and in most frequency bands with terrestrial radio systems. The most useful orbit for communication satellites is the geostationary orbit, and the signal channels between satellite and control earth stations required for these functions are carried by radio subsystems. Margin of power is provided in addition to ensure that channel performance targets are reached. Communication satellites are designed to relay several signals simultaneously. And satellite communications are capable of long-distance communications and can be operated with mobile terrestrial terminals.

Broadcasting

Broadcasting has been a use case for geosynchronous satellites for almost as long as satellites have been in the geosynchronous orbit. These satellites have been used for direct-broadcast satellite television, in which the satellite sent transmission directly to a home. Previous to the popularity of direct-broadcast television, these satellites were used to transmit signals for conventional broadcasting.

As broadcasting has changed and the use of satellites in broadcasting has continued, hybrid satellite systems have been used to offer radio access systems capable of providing both terrestrial and satellite connectivity. Practical examples of the existing hybrid systems, such as digital video broadcasting-satellite services to handheld devices, have been used.

The main focus in these types of satellite systems is in solving spectrum challenges between the terrestrial and satellite components.

Navigation

One of the most well-known use cases of GEO satellites is the satellite-based navigation system, which is used to localize a radio receiving terminal, also referred to as the global positioning system (GPS). All GPS satellites share the same frequency bands, making use of the code division multiple access (CDMA) technique.

Weather forecasting

Geosynchronous satellites are also used for weather forecasting. These satellite systems have unique characteristics and are capable of producing different products. These geostationary satellites spin at the same rate of the Earth and are capable of constantly focusing on the same area. This enables the satellite to take pictures of the Earth at the same location every thirty minutes.

Global Positioning Systems

The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment. The U.S. Space Force develops, maintains, and operates the space and control segments.

The Global Positioning System (GPS), originally Navstar GPS, is a satellite-based radionavigation system owned by the United States government and operated by the United States Space Force.

It is a technology by which the location of an object, its velocity, direction, altitude and time can be known precisely at any time, irrespective of day/night, weather, or the configuration of the object.

History of GPS

GPS, originally named NAVSTAR - Navigation System with Time and Ranging was introduced by the United States Department of Defence in 1987. The full constellation of 24 satellites became operational in 1994 and was later launched for civilian use in the 1980s.

Today, GPS is a multi-use, space-based radionavigation system owned by the US Government and operated by the United States Air Force to meet national defense, homeland security, civil, commercial, and scientific needs.

GPS currently provides two levels of service: Standard Positioning Service (SPS) which uses the coarse acquisition (C/A) code on the L1 frequency, and Precise Positioning Service (PPS) which uses the P(Y) code on both the L1 and L2 frequencies. Access to the PPS is restricted to US Armed Forces, US Federal agencies, and selected allied armed forces and governments. The SPS is available to all users on a continuous, worldwide basis, free of any direct user charges.

Segments of GPS

GPS satellites fly in Medium Earth Orbit (MEO) at an altitude of approximately 20,200 km (12,550 miles). Each satellite circles the Earth twice a day. The **space segment** of GPS consists of 24 main satellites & 8 backup satellites placed in near circular orbits, arranged in 6 orbital planes, with 55 degree inclination to equator. The period of revolution is 12 hrs, thus there are at least 4 satellites available for observation every time worldwide.

The GPS **control segment** consists of a global network of ground facilities that track the GPS satellites, monitor their transmissions, perform analyses, and send commands and data to the constellation. The current Operational Control Segment (OCS) includes a master control station, an alternate master control station, 11 command and control antennas, and 16 monitoring sites.

User Segment:

- GPS technology is now in everything from cell phones and wristwatches to bulldozers, shipping containers, and ATM's.
- Major communications networks, banking systems, financial markets, and power grids depend heavily on GPS for precise time synchronization.
- GPS boosts productivity across a wide swath of the economy, to include farming, construction, mining, surveying, package delivery, and logistical supply chain management.
- GPS saves lives by preventing transportation accidents, aiding search and rescue efforts, and speeding the delivery of emergency services and disaster relief.
- GPS also advances scientific aims such as weather forecasting, earthquake monitoring, and environmental protection.
- GPS remains critical to U.S. national security, and its applications are integrated into virtually every facet of U.S. military operations. Nearly all new military assets -- from vehicles to munitions -- come equipped with GPS.

Applications of GPS

Time Synchronization

In addition to longitude, latitude, and altitude, the Global Positioning System (GPS) provides a critical fourth dimension – time. Each GPS satellite contains multiple atomic clocks that contribute very precise time data to the GPS signals. GPS receivers decode these signals, effectively synchronizing each receiver to the atomic clocks. This enables users to determine the time to within 100 billionths of a second, without the cost of owning and operating atomic clocks.

- Widespread availability of atomic clock time, without the atomic clocks.
- Precise synchronization of communications systems, power grids, financial networks, and other critical infrastructure.
- More efficient use of limited radio spectrum by wireless networks.
- Improved network management and optimization, making traceable time tags possible for financial transactions and billing.

- Communication of high-precision time among national laboratories using "common view" techniques.

There is an unknown offset between the satellite clocks and the receiver clock that introduces a corresponding offset in the distance calculation. Because of this offset, the measured distance is called a **pseudorange**.

Public Safety & Disaster Relief

A critical component of any successful rescue operation is time. Knowing the precise location of landmarks, streets, buildings, emergency service resources, and disaster relief sites reduces that time -- and saves lives. This information is critical to disaster relief teams and public safety personnel in order to protect life and reduce property loss.

Industrial Economy

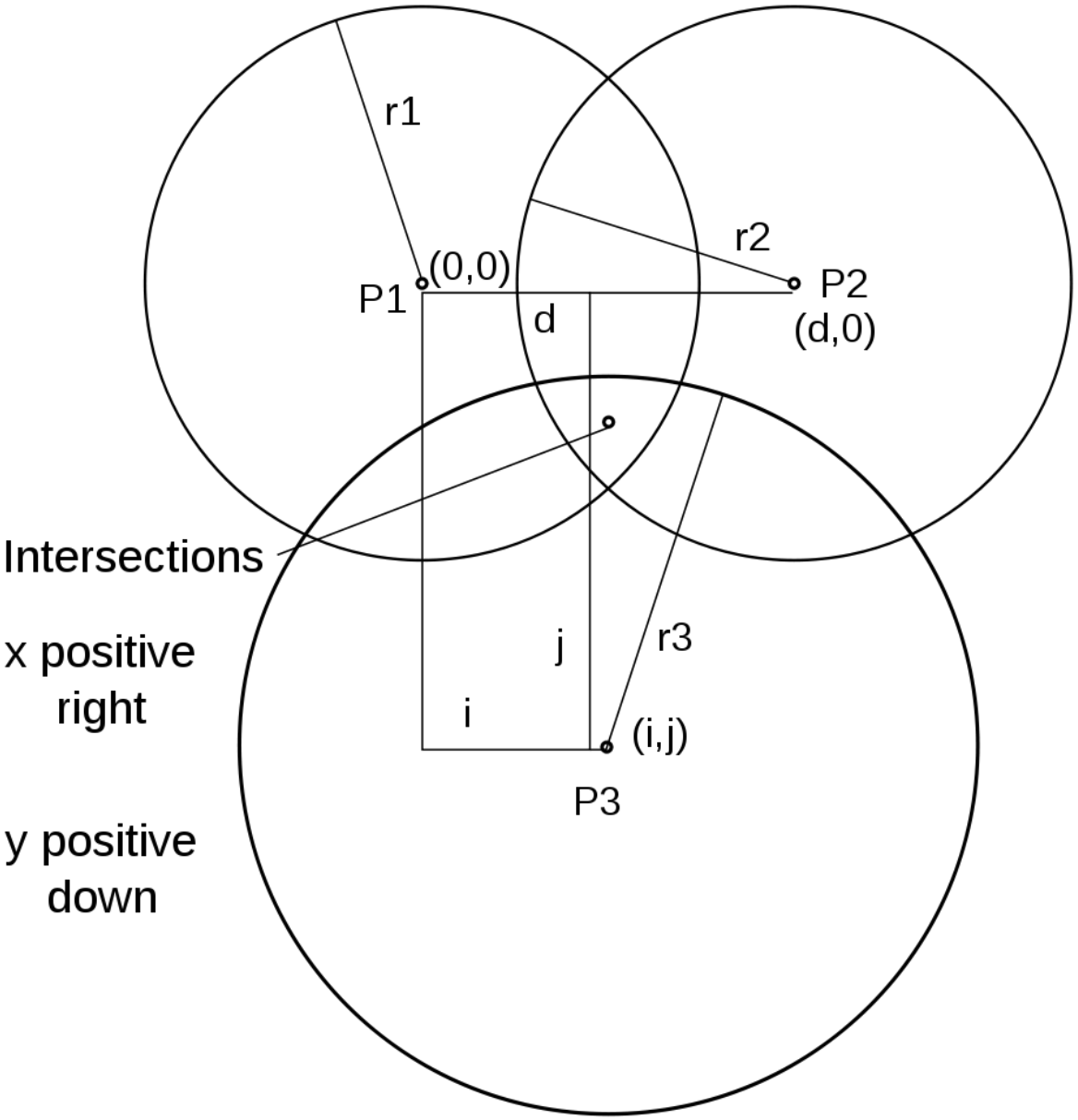
GPS boosts productivity across a wide swath of the economy, to include farming, construction, mining, surveying, package delivery, and logistical supply chain management. Major communications networks, banking systems, financial markets, and power grids depend heavily on GPS for precise time synchronization. Some wireless services cannot operate without it.

Working of GPS

Position fix is obtained in passive receivers by the triangulation method. Estimated ranges from four satellites are used to derive the position and altitude of a point. Ranges from three satellites can provide the latitude and longitude of a point on the Earth. The addition of a fourth satellite can provide a user's altitude and correct receiver clock error.

Trilateration a.k.a True-range multilateration is a method to determine the location of a movable vehicle or stationary point in space using multiple ranges (distances) between the vehicle/point and multiple spatially-separated known locations (often termed 'stations'). Energy waves may be involved in determining range, but are not required.

For Example, on a plane, if we know our distance from three points, we know exactly where we are. Let us say that we are 10 miles away from point A, 12 miles away from point B, and 15 miles away from point C. If we draw three circles with the centers at A, B, and C, we must be somewhere on circle A, somewhere on circle B, and somewhere on circle C. These three circles meet at one single point (if our distances are correct), our position.



In three-dimensional space, we need at least four spheres to find our exact position in space, i.e., longitude, latitude, and altitude. However, if we have additional facts about our location (for example, we know that we are not inside the ocean or somewhere in space), three spheres are enough, because one of the two points, where the spheres meet, is so improbable that the other can be selected without a doubt.

Distance Measurement with GPS

Measuring the distance is done using a principle called one-way ranging. Each of 24 satellites synchronously transmits a complex signal each having a unique pattern. The computer on the receiver measures the delay between the signals from the satellites and its copy of signals to determine the distances to the satellites.

Synchronization with GPS

The satellites' clocks are synchronized with each other and with the receiver's clock. Satellites use atomic clocks that are precise and can function synchronously with each other. The receiver's clock however, is a normal quartz clock (an atomic clock costs more that $50,000), and there is no way to synchronize it with the satellite clocks.

There is an unknown offset (same for all satellites being used) between the satellite clocks and the receiver clock that introduces a corresponding offset in the distance calculation. Because of this offset, the measured distance is called a pseudorange. The calculation of position becomes finding four unknowns: the Xp, Yp, Zp coordinates of the receiver, and common clock offset dt. For finding these four unknown values, we need at least four equations, from the four connected satellites.

$$PR_1 = \frac{1}{2}[(x_1 - x_r)^2 + (y_1 - y_r)^2 + (z_1 - z_r)^2] + c.\,dt$$

$$PR_2 = \frac{1}{2}[(x_2 - x_r)^2 + (y_2 - y_r)^2 + (z_2 - z_r)^2] + c.\,dt$$

$$PR_3 = \frac{1}{2}[(x_3 - x_r)^2 + (y_3 - y_r)^2 + (z_3 - z_r)^2] + c.\,dt$$

$$PR_4 = \frac{1}{2}[(x_4 - x_r)^2 + (y_4 - y_r)^2 + (z_4 - z_r)^2] + c.\,dt$$

The coordinates used in the above formulas are in an Earth-Centered Earth-Fixed (ECEF) reference frame, which means that the origin of the coordinate space is at the center of the Earth and the coordinate space rotates with the Earth. This implies that the ECEF coordinates of a fixed point on the surface of the earth do not change.

Global navigation satellite system

GNSS is a general term describing any satellite constellation that provides positioning, navigation, and timing (PNT) services on a global or regional basis. While GPS is the most prevalent GNSS, other nations are fielding, or have fielded, their own systems to provide complementary, independent PNT capability.

- BeiDou Navigation Satellite System (BDS)
- Galileo
- GLONASS
- IRNSS / NavIC
- Quasi-Zenith Satellite System (QZSS)

Global System for Mobile Communications (GSM)

What is GSM?

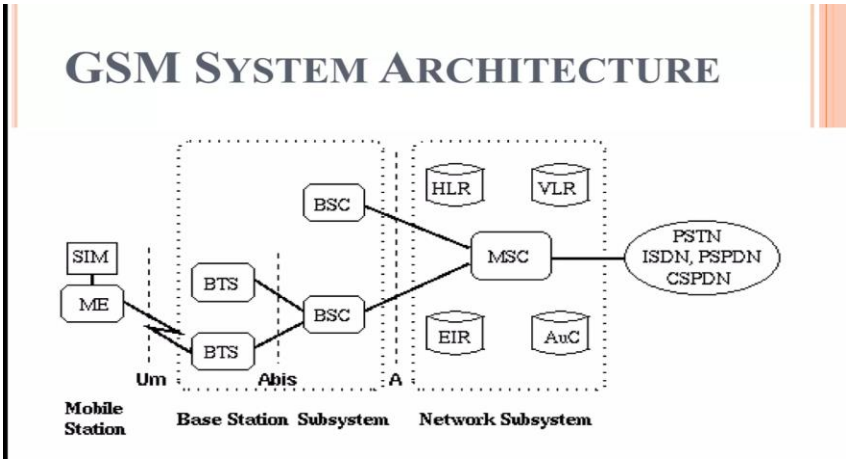
- GSM stands for Global System for Mobile Communication.
- GSM is an open and digital cellular technology used for mobile communication.
- It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz .
- It uses the combination of FDMA and TDMA.
- 2G technology
- Standard developed by ETSI
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

Features of GSM are :

- Supports international roaming
- Clear voice clarity
- Ability to support multiple handheld devices.
- Low powered handheld devices.
- Ease of accessing network
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services
- Support for new services
- Low-cost mobile sets and base stations (BSs)
- Subscriber Identity Module (SIM) :
    - One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card.
    - The SIM is a detachable smart card containing a user's subscription information and phone book.
    - This allows users to retain their information after switching handsets.

- Phone locking
    - Sometimes mobile network operators restrict handsets that they sell for exclusive use in their own network.
    - This is called SIM locking and is implemented by a software feature of the phone.
    - A subscriber may usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or use software and websites to unlock the handset themselves.

GSM ARCHITECTURE:



- The GSM network can be broadly divided into −
  - The Mobile Station (MS)
  - The Base Station Subsystem (BSS)
  - The Network Switching Subsystem (NSS)
  - The Operation Support Subsystem (OSS)

- **GSM - The Mobile Station**
  - The MS consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card.
  - It provides the air interface to the user in GSM networks.

The MS Functions

- **GSM - The Base Station Subsystem (BSS)**
  - The BSS is composed of two parts −
    - The Base Transceiver Station (BTS)
    - The Base Station Controller (BSC)
  - The BTS and the BSC communicate across the specified Abis interface, enabling operations between components that are made by different suppliers.
  - The BSS uses the Abis interface between the BTS and the BSC.
  - **The Base Transceiver Station (BTS)**
    - The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the MS.
    - The BTS corresponds to the transceivers and antennas used in each cell of the network.
    - A BTS is usually placed in the center of a cell.

        - Each BTS serves as a single cell. It also includes the following functions −
            - Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
            - Time and frequency synchronizing
    - **The Base Station Controller (BSC)**
        - The BSC manages the radio resources for one or more BTSs
        - The BSC is the connection between the mobile and the MSC
        - The BSC also translates the 13 Kbps voice channel used over the radio link to the standard 64 Kbps channel used by the Public Switched Telephone Network (PSDN) or ISDN.
        - It is a switching device that handles the radio resources.
        - Performs traffic concentration to reduce the number of lines from the MSC
- **The Network Switching Subsystem (NSS)**
    - The Network switching system (NSS), the main part of which is the Mobile Switching Center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as authentication.
    - **Home Location Register (HLR)**
        - The HLR is a database used for storage and management of subscriptions.
        - The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status.
        - When an individual buys a subscription in the form of SIM, then all the information about this subscription is registered in the HLR of that operator.
    - **Mobile Services Switching Center (MSC)**
        - The central component of the Network Subsystem is the MSC.
        - The MSC performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber.
    - **Visitor Location Register (VLR)**
        - The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers.
        - When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR.
    - **Authentication Center (AUC)**
        - The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.
    - **Equipment Identity Register (EIR)**

- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS.

- **The Operation Support Subsystem(OSS):**
  - The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS).

  - Here are some of the OMC functions:
    1,Administration and commercial operation (subscription, end terminals, charging and statistics).

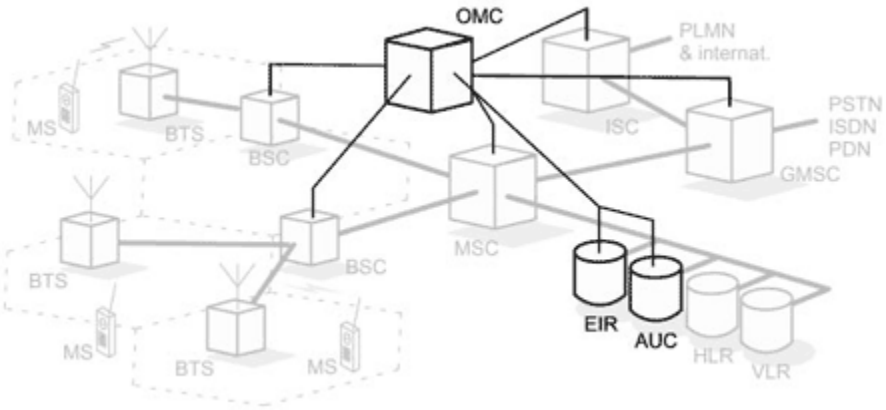
    2,Security Management.

    3,Network configuration, Operation and Performance Management.

    4,Maintenance Tasks.

The operation and Maintenance functions are based on the concepts of the Telecommunication Management Network (TMN), which is standardized in the ITU-T series M.30.

Following is the figure, which shows how the OMC system covers all the GSM elements.



The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

Interfaces:

Three subsystems **BSS**, **NSS** and **OSS** are connected with each other via some interfaces. Total three interfaces are there:

- **Air Interface**: Air interface is also known as UM interface. Interface between MS and BTS is called the UM interface because it is a mobile analog to the U interface of ISDN. It uses TDMA

- **Abis Interface** : It is a BSS internal interface linking with BTS and BSC.I is based on LAP (Link Access Protocol)

- **A interface** : It provides communication between BSS and MSC

Multiplexing:

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

An efficient system maximizes the utilization of all resources; bandwidth is one of the most precious resources we have in data communications

Figure 6.1 *Dividing a link into channels*

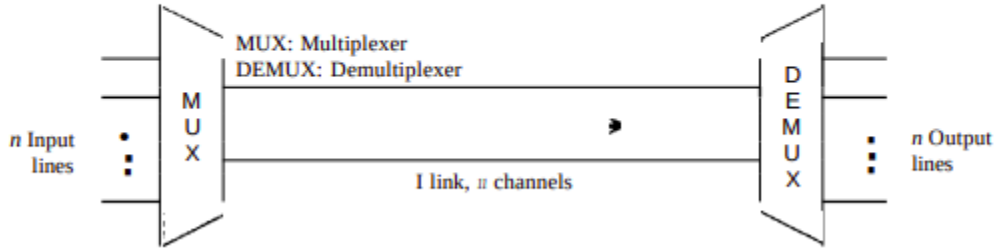
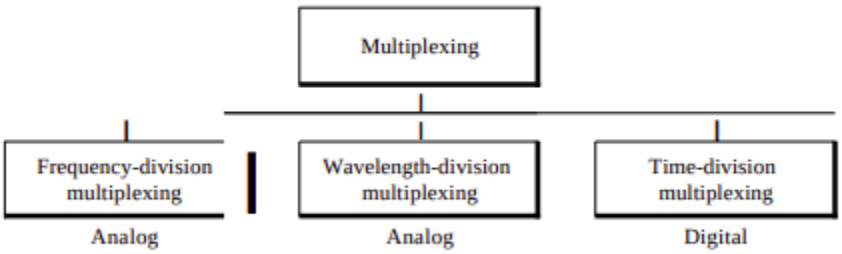


Figure 6.2 *Categories of multiplexing*

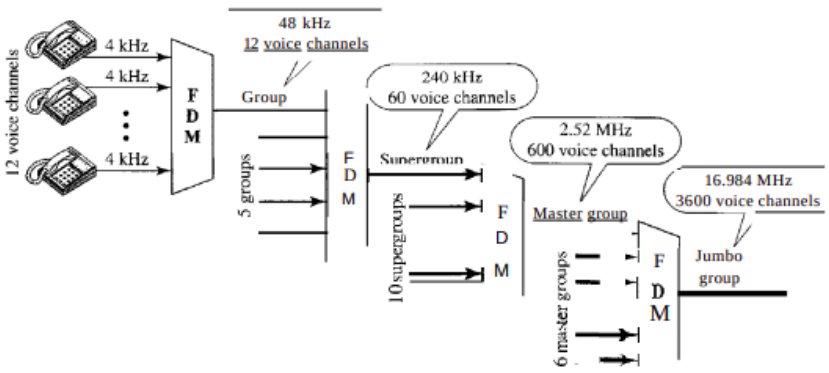


FDMA(Frequency-division multiple access)

FDMA is a type of channelization protocol. This bandwidth is divided into various frequency bands. Each station is allocated with band to send data and that band is reserved for particular station for all the time which is as follows
:The frequency bands of different stations are separated by small bands of unused frequency and that unused frequency bands are called guard bands that prevent the interference of stations. It is like an access method in the data link layer in which the data link layer at each station tells its physical layer to make a band pass signal from the data passed to it. The signal is created in the allocated band and there is no physical multiplexer at the physical layer

It was primarily used in 1G and PSTN

Figure 6.9 *Analog hierarchy*



TDMA(Time Division Multiple Access)

TDMA is the channelization protocol in which bandwidth of a channel is divided into various stations on the time basis. There is a time slot given to each station, the station can transmit data during that time slot only which is as follows :
Each station must be aware of its beginning time slot and the location of the time slot. TDMA requires synchronization between different stations. It is a type of access method in the data link layer. At each station data link layer tells the station to use the allocated time slot.

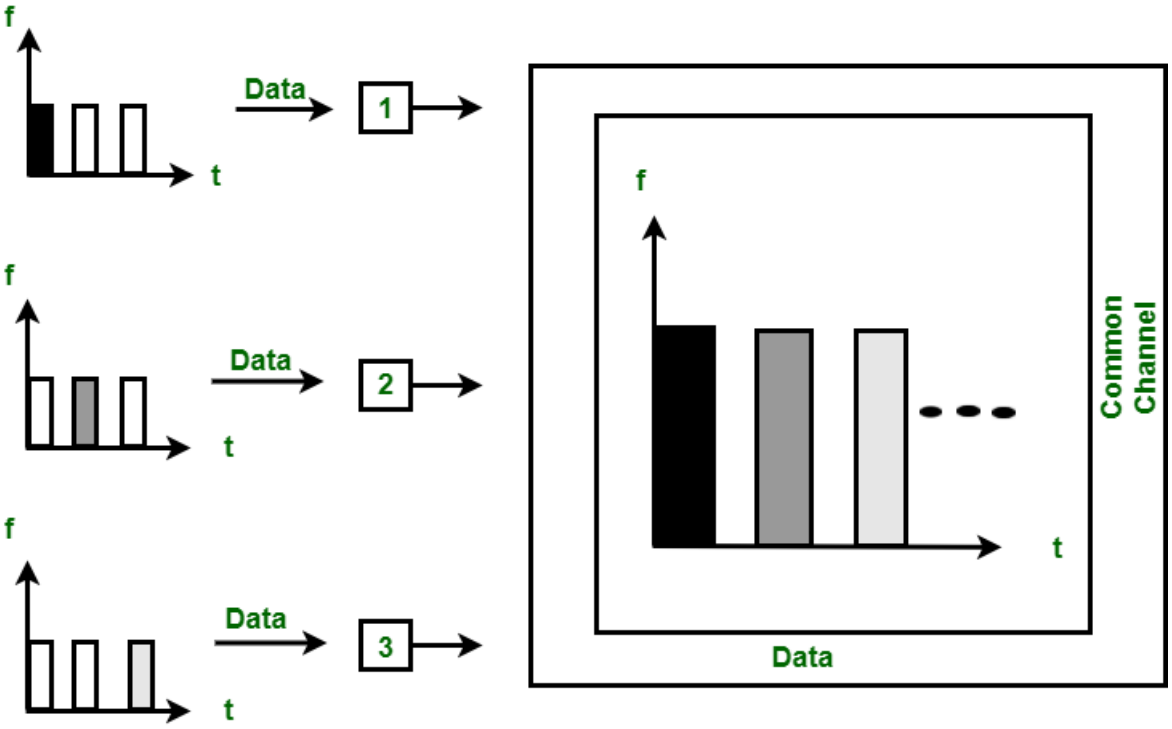
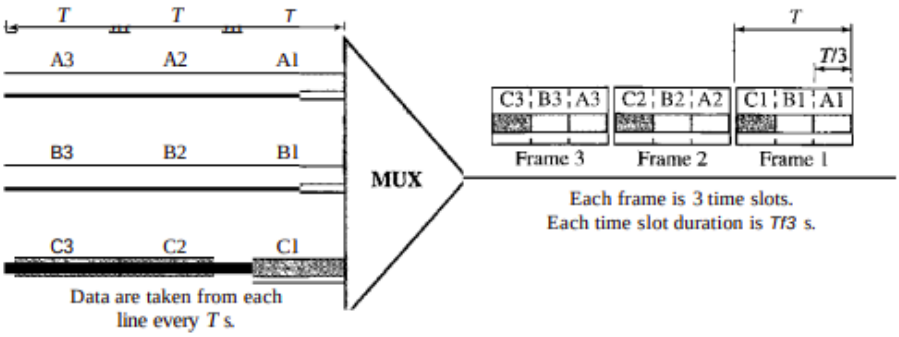


Figure 6.13 *Synchronous time-division multiplexing*



PSTN :

PSTN stands for Public Switched Telephone Network. PSTN connects with MSC. PSTN originally a network of fixed line analog telephone systems. Now almost entirely digital in its core network and includes mobile and other networks as well as fixed telephones. The earlier landline phones which are at our home are nothing but PSTN. They are circuit switched networks.

This is the system that has been in general use since the late 1800s. It's the aggregation of circuit-switching telephone networks that has evolved from the days of Alexander Graham Bell.

Using underground copper wires, this legacy platform has provided businesses and households alike with a reliable means to communicate with anyone around the world for generations. Today, it is almost entirely digit

Circuit Switching :

The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established

In-circuit switching has there are 3 phases:
i) Connection Establishment.
ii) Data Transfer.
iii) Connection Released.

Advantages:
1,The main advantage of circuit switching is that a committed transmission channel is established between the computers which give a guaranteed data rate.
2,In-circuit switching, there is no delay in data flow because of the dedicated transmission path.

Disadvantages:
1,It takes a long time to establish a connection.
2,More bandwidth is required in setting up dedicated channels.
3,It cannot be used to transmit any other data even if the channel is free as the connection is dedicated to circuit switching.

Advantages Of GSM:

- The GSM based networks (i.e. base stations) are deployed across the world and hence the same mobile phone works across the globe.
- Advanced versions of GSM with a higher number of antennas will provide high speed download and upload of data.
- The phone works based on a SIM card and hence it is easy to change the different varieties of phones by users.

Disadvantages Of GSM:

- GSM provides limited data rate capability, for higher data rate GSM advanced version devices are used.
- In order to increase the coverage, repeaters are required to be installed.

GPRS – OVERVIEW

General Packet Radio System is also known as **GPRS** is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) usersget benefit from this system, as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications, which continues to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structural way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

In the current versions of GPRS, networks based on the Internet Protocol (IP) like the globalinternet or private/corporate intranets and X.25 networks are supported.

Who Owns GPRS?

The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

Key Features

Following three key features describe wireless packet data:

- **Always online feature -** Removes the dial-up process, making applications only oneclick away.
- **Upgrade to existing systems -** Operators do not need to replace their equipment;rather, GPRS is added on top of the existing infrastructure.
- **An integral part of future 3G systems -** GPRS is the packet data core network for3G systems **EDGE** and **WCDMA**.

Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- Open architecture
- Consistent IP services
- Same infrastructure for different air interfaces
- Integrated telephony and Internet infrastructure
- Leverage industry investment in IP
- Service innovation independent of infrastructure

Benefits of GPRS

Higher Data Rate

GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process, and equally rates for data permission are restrained to 9.6 kbps. The session establishment time offered whileGPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbps.

Easy Billing

GPRS packet transmission offers a more user-friendly billing than that of circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with busty traffic. The user must pay for the entire airtime, even for the idle periods when no packet has been sent (e.g., when the user reads a Web page).

In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume only.

2. GPRS – APPLICATIONS

GPRS has opened a wide range of unique services to the mobile wireless subscribers.

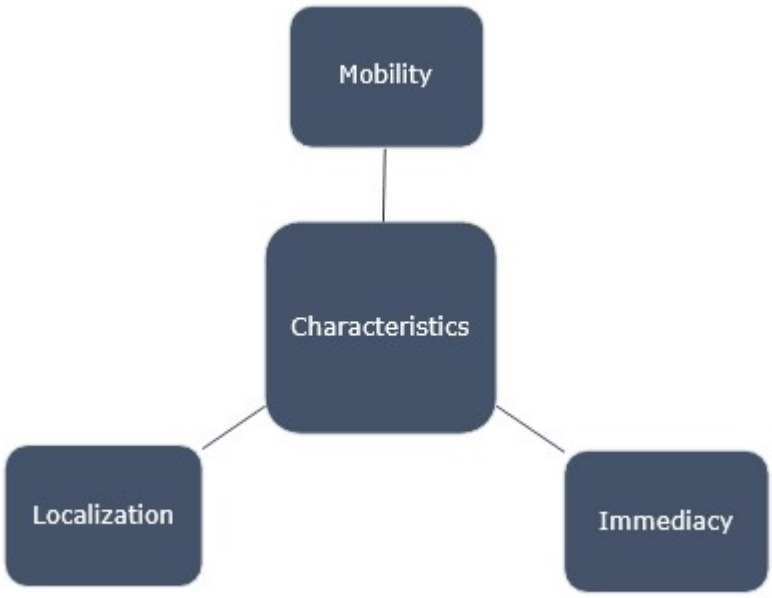
Characteristics of GPRS

Following is some of the characteristics that have opened a market full of enhanced value services to the users:

- **Mobility -** The ability to maintain constant voice and data communications while on the move.

- **Immediacy -** Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.

- **Localization -** Allows subscribers to obtain information relevant to their current location.



Using the above three characteristics, varied possible applications are being developed for the mobile subscribers. These applications, in general, can be divided into two high-level categories:

- **Corporation**
- **Consumer**

These two levels further include:

- **Communications -** E-mail, fax, unified messaging, and intranet/internet access, etc.
- **Value-added services -** Information services, games, etc.
- **E-commerce -** Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications -** Navigation, traffic conditions, airline/rail schedules, location finder, etc.
- **Vertical applications -** Freight delivery, fleet management, and sales-force automation.
- **Advertising -** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

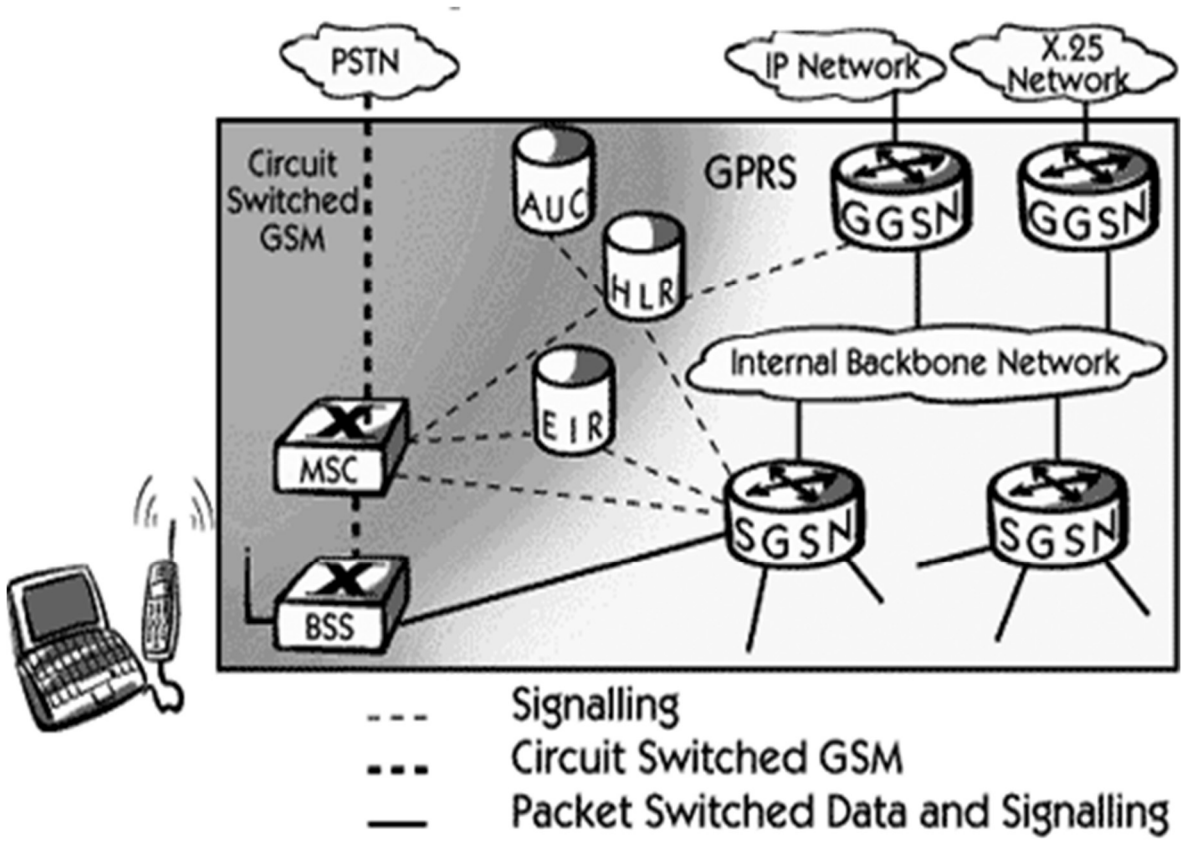
Along with the above applications, non-voice services such as SMS, MMS, and voice calls are also possible with GPRS. Closed User Group (CUG) is a common term used after GPRS is in the market. In addition, it is planned to implement supplementary services, such as Call Forwarding Unconditional (CFU), and Call Forwarding on Mobile subscriber Not Reachable (CFNRc), and Closed User Group (CUG).

3. GPRS – ARCHITECTURE

GPRS architecture works on the same procedure like GSM network, but it has some additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates of 9.6 to 171 kbps. Along with the packet data transport, the GSM network accommodates multiple users to share the same air interface resources concurrently.

GPRS Architecture Diagram

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required. The architecture diagram of GPRS is as follows:



Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station *MS*	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSMfor voice calls.
BTS	A software upgrade is required in the existing BaseTransceiver Station *BTS*.
BSC	The Base Station Controller *BSC* requires a software upgrade and the installation of new hardware called the packet controlunit *PCU*. The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
Databases *HLR*, *VLR*, *etc*.	databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.
GPRS Support Nodes *GSNs*	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node SGSN and gateway GPRS support node GGSN.

GPRS Mobile Stations

New Mobile Stations *MS* are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speedversion of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units *PCUs* and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem *BSS* for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over theair interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call.
However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center *MSC* per standard GSM, and data is sent to a new device called the SGSN via the PCU over aFrame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes *GSNs* and, Serving GPRSSupport Node *SGSN* are added:

Gateway GPRS Support Node GGSN

The Gateway GPRS Support Node acts as an interface and a router to external networks. It containsrouting information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging informationconnected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node SGSN

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signaling from a GSN to a MSC, HLR or EIRis done using SS7.

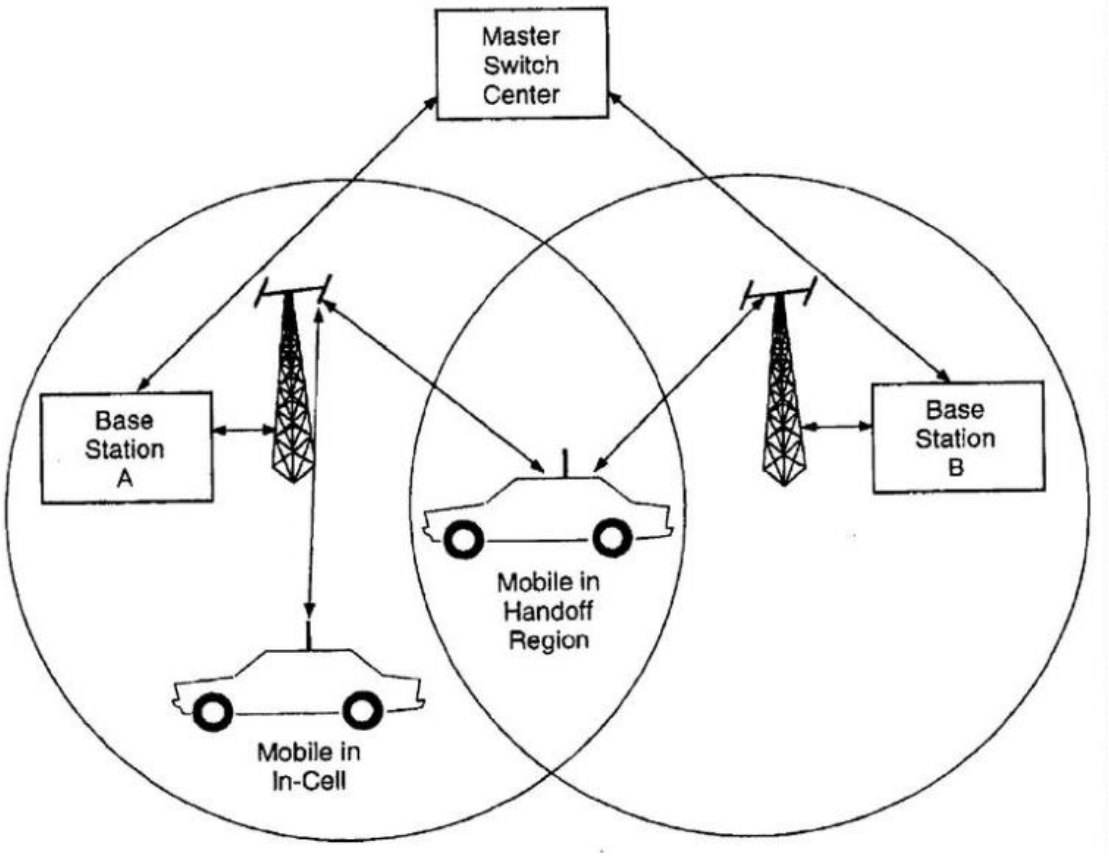
Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM,except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

Handoff

It may happen that, during a conversation, the mobile station moves from one cell to another. When it does, the signal may become weak. To solve this problem, the MSC monitors the level of the signal every few seconds. If the strength of the signal diminishes, the MSC seeks a new cell that can better accommodate the communication. The MSC then changes the channel carrying the call (hands the signal off from the old channel to a new one).

The terms handover or handoff refers to the process of transferring ongoing call or data connectivity from one Base Station to other Base Station. When a mobile moves into the different cell while the conversation is in progress then the MSC (Mobile Switching Centre) transfer the call to a new channel belonging to the new Base Station.



Need for Handoff

- As the user (MS) moves away from the cell of one tower (BS), the signal strength of that BS reduces. However, the signal from another (now closer) BS grows, and a handoff is imminent.
- One of the building blocks of cellular communication is mobility, which refers to providing users with the freedom of movement while they still are connected to the network.

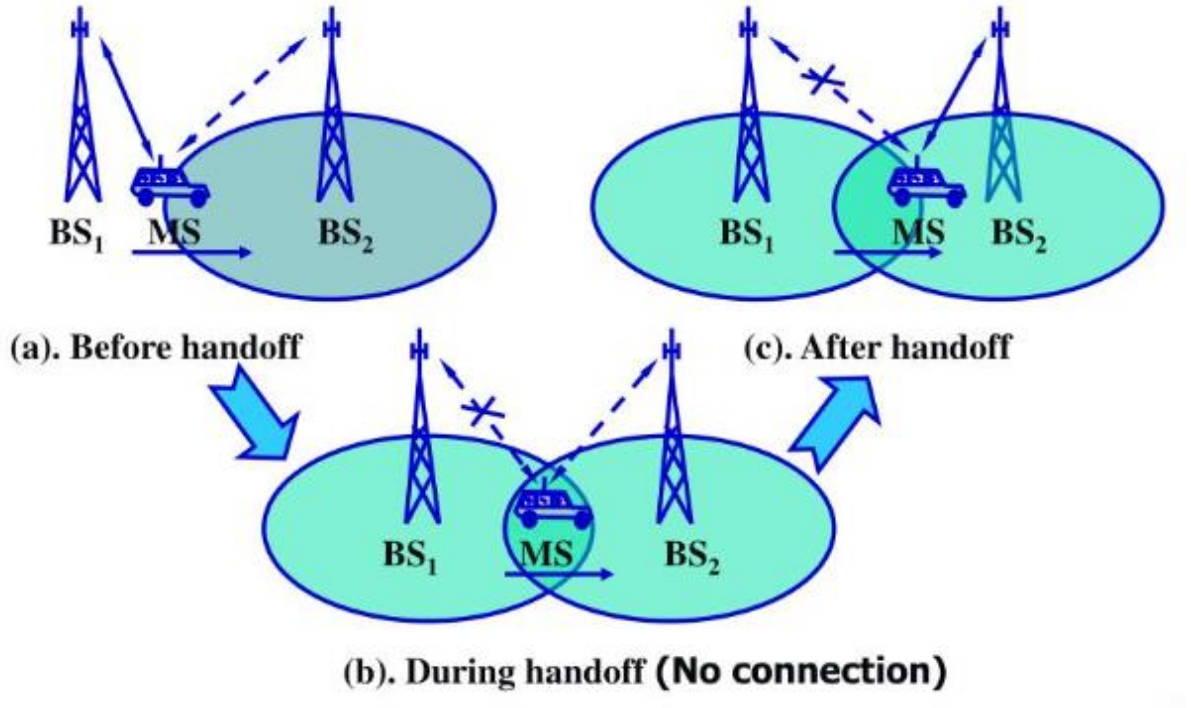
- One of the building blocks of cellular communication is mobility, which refers to providing users with the freedom of movement while they still are connected to the network.
- If a MS who is in a call or a data session moves out of coverage of one cell and enters coverage area of another cell, a handoff is triggered for a continuum of service
- Each cell has a pre-defined capacity, i.e. it can handle only a specific number of MS. If the number of users using a particular cell reaches its maximum capacity, then a handoff occurs. Some of the calls are transferred to adjoining cells, provided that the MS is in the overlapping coverage area of both the cells.

Type of Handoff

1. Hard handoff
2. Soft handoff

Hard Handoff

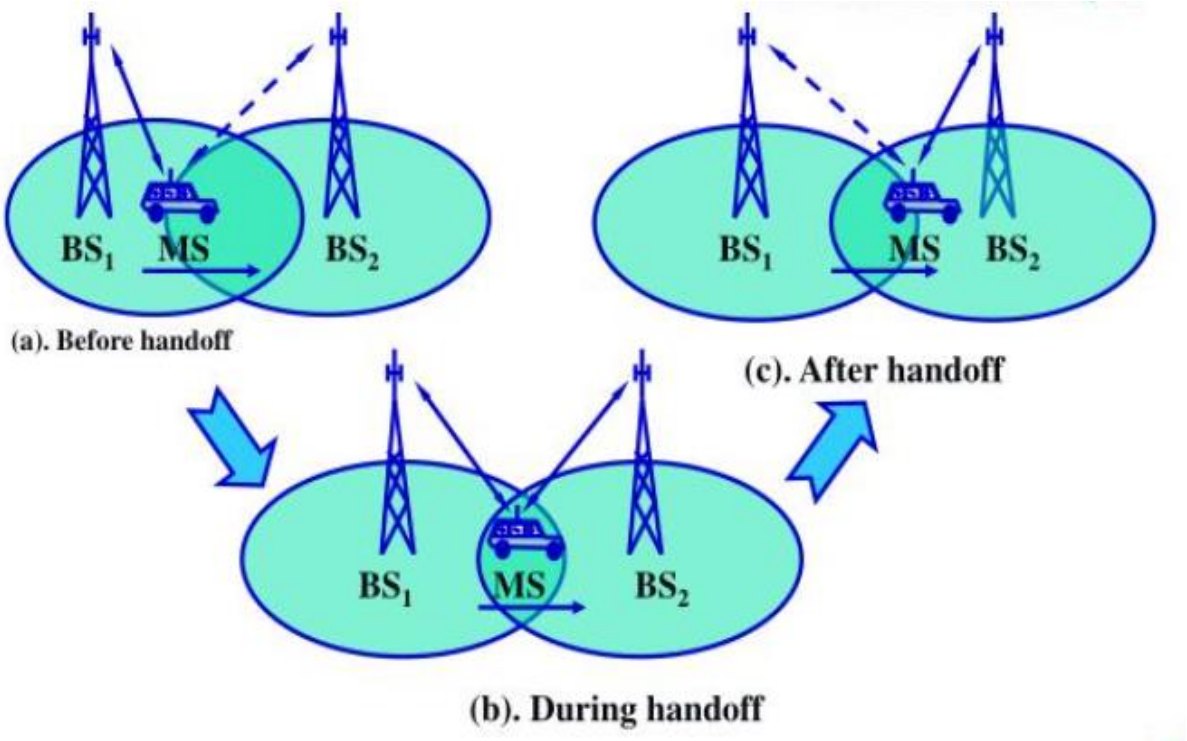
Hard Handoff is a technique that requires the user's connection to be broken before connecting to another while switching between two BTS and hence is equivalent to "breaking before making". There is no burden on the Base Station and MSC because the switching takes place so quickly that it can hardly be noticed by the users. There is no connection when breaking the connection because of that there is slight disturbance almost negligible



Soft Handoff

Systems use a soft handoff. In this case, a mobile station can communicate with two base stations at the same time. This means that, during handoff, a mobile station may continue with the new base station before breaking off from the old one.

In Soft Handoff, at least one of the links is kept when radio signals are added or removed to the Base Station. Soft Handoff adopted the 'make before break' policy. Soft Handoff is more costly than Hard Handoff.



Difference between Hard and Soft Handoff

Hard Handoff	Soft Handoff
It is defined as hand-off where an existing connection must be broken when the new one is established.	It is defined as hand-off where a new connection is established before old one is released.
Only one connection at a time (some time no connection)	Always have at least one or more connection at a time
Slight Disturbance	No disturbance
Less complex when compared to soft hand-off.	It is more complex than hard hand-off.
Cheaper in cost	Cheaper in cost
It allocates different frequency.	It allocates same frequency.

IEEE 802.11 WLAN Standards

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipment that are connected to the wireless LAN. A station can be of two types:

- **Wireless Access Points (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client.** − Clients are workstations, computers, laptops, printers, smartphones, etc.

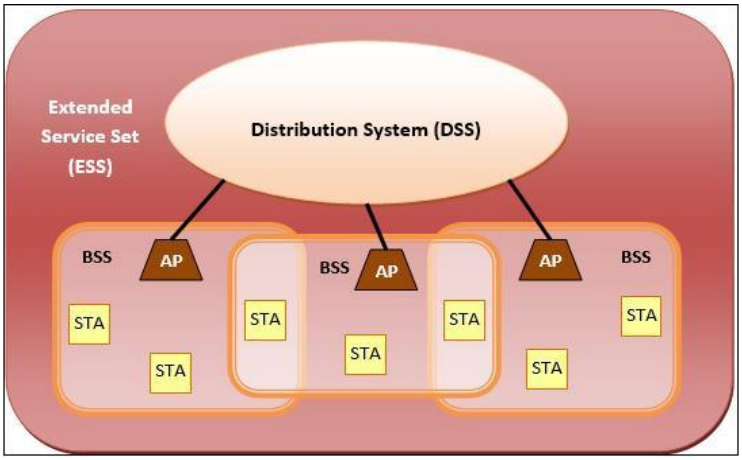
Each station has a wireless network interface controller.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- **Infrastructure BSS** − Here, the devices communicate with other devices through access points.
- **Independent BSS** − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.



Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

IEEE 802.11 WLAN Standards

IEEE 802.11

IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

IEEE 802.11a

802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11. It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code. As 2.4 GHz

band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

IEEE 802.11b

802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band. It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs. However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.

Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.

IEEE 802.11g

802.11g was indorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a). It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

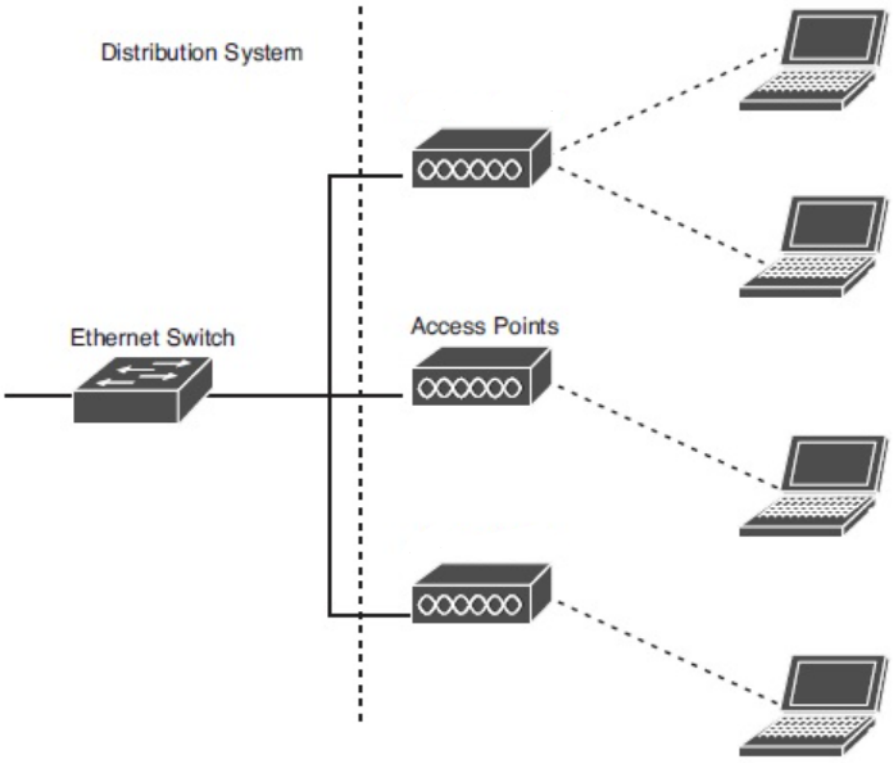
IEEE 802.11n

802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps. It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

Standard	Year	Frequency Band	Speed	Modulation	Characteristics
802.11	1997	2.4GHz	1-2Mbps	DSSS,FHSS	Base version
802.11b	1999	2.4GHz	11Mbps	DSSS	Oldest, least expensive
802.11a	1999	5 GHz	54Mbps	OFDM	Rarely used
802.11g	2003	2.4 GHz	54Mbps	OFDM	Compatible with 802.11b networks
802.11n	2009	2.4GHz 5 GHz	65-600Mbps	OFDM	- Backward compatible with 802.11a, b, g standards - MIMO (multiple input-multiple output) - Channel bonding: doubles the bandwidth - Frame aggregation : reduces overhead
802.11ac	2014	5 GHz	Up to 7 Gigabit	MIMO-OFDM	- Gigabit Wi-Fi - MU-MIMO (Multi User MIMO) - Wave 1 (2014) vs. Wave 2 (2016)

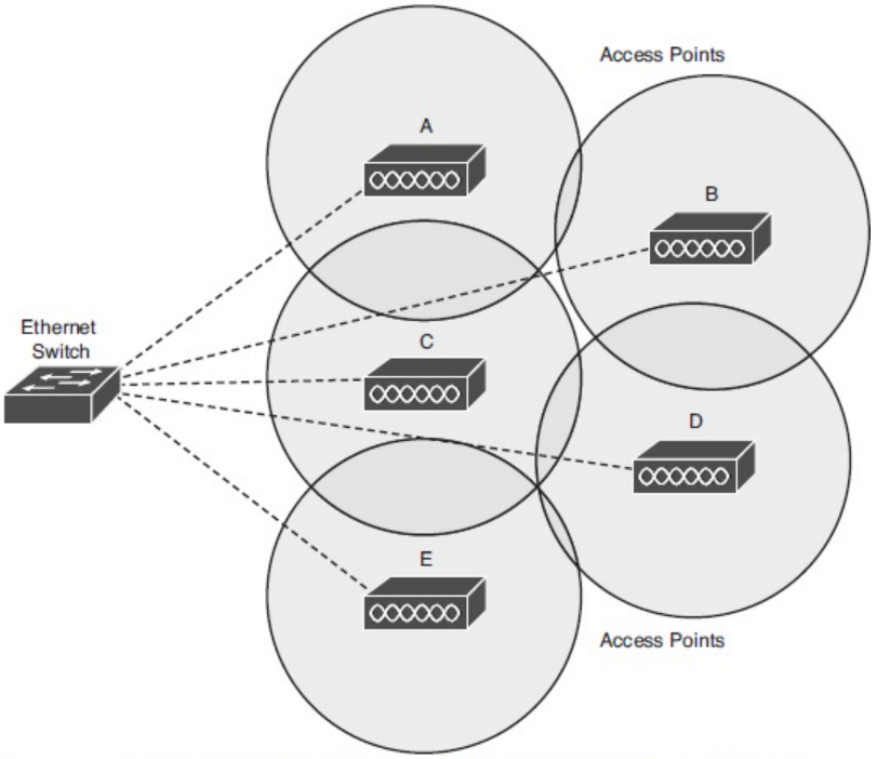
Infrastructure based WLAN

Most companies, public hotspots, and homeowners implement infrastructure WLANs. An infrastructure WLAN, offers a means to extend a wired network.
In infrastructure mode, the WLAN network is composed of stations as well as one or more access points(APs). The device access point is like a base station used in cellular systems. All the communications between stations will go through an access point.
Each access point forms a radio cell, also called a basic service set (BSS), which enables wireless users located within the cell to connect to the access point. This allows users to communicate with other wireless users, as well as with servers and network applications connecting to the distribution system.
The wireless WLAN network with one AP is referred to as BSS(Basic Service Set). When more than one APs are available in a network to form a sub-network, it is referred as ESS(Extended Service Set).



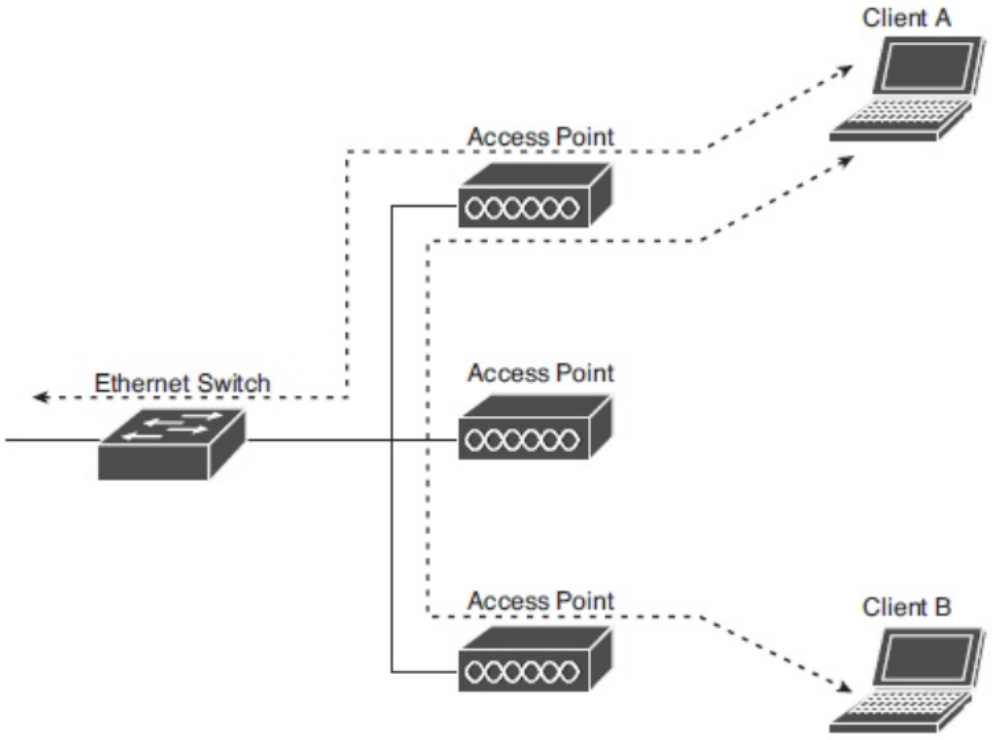
An Infrastructure Wireless LAN Interfaces Client Devices to a Wired Distribution System and Extends Coverage Through Use of Access Points

If access points with overlapping radio cells are installed, as shown in figure below , then users can roam throughout the facility without any noticeable loss of connectivity.The radio card within the user's mobile device will automatically re-associate with access points having stronger signals. For example, a user might begin downloading a file when associated with access point A. As the user walks out of range of access point A and within range of access point B, the client radio automatically re-associates the user to access point B and continues the downloading of the file through access point B. The user generally does not experience any noticeable delays, but voice over WLAN phones might drop connections if the roaming delay exceeds 150 milliseconds.



Multicell Wireless LAN with Overlapping Cells Supports Roaming

In infrastructure WLANs, data transmissions do not occur directly between the wireless clients. Data traffic going from one wireless user to another user must travel through an access point as shown in below figure. The access point receives the data traffic going from client A to client B, for example, and retransmits the data to client B. As a result, significant data traffic between wireless users decreases throughput because of the access point needing to relay the data to the destination user. If the source wireless user is sending data to a node on the distribution system, then the access point does not need to retransmit the data to other wireless users.



Typical Flow of Data Through an Infrastructure Wireless LAN

Intrusion Handling

Definition of intrusion

The act of intruding or the state of being intruded especially the act of wrongfully entering upon, seizing, or taking possession of the property of another is called intrusion and the person doing this act called intruder.

Intruders

Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

Intruders are divided into three categories:

- **Masquerader:** The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.
- **Misfeasor:** The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.
- **Clandestine User:** The category of individuals those have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Below are the different ways adopted by intruders for cracking passwords for stealing confidential information:

- Regressively try all short passwords that may open the system for them.
- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.

- Try unlocking the system by personal information of the user such as their name, family member names, address, phone number in different combinations.
- Making use of Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, locality info.

To prevent intruders from attacking the computer system, it is extremely important to be aware of the preventive measures which leads to strengthening of the security posture.

Approaches to Intrusion Detection and Prevention:

1. Pre-emptive Blocking:

It is also called Banishment vigilance. It seeks to prevent intrusion from happening before they occur. The above method is done by observing any danger signs of imminent threats and then blocking user or IP address from which these signs originate. Example – This technique includes attempts to detect early foot-printing of an imminent intrusion then blocking IP or user that is source of foot-printing activity. If Admin finds that particular IP address is source of frequent port scans and other scans of their system then they will block that IP address at firewall. The above intrusion detection and avoidance can be quite complicated which could potentially block legitimate user by mistake. The complexity arises from distinguishing legitimate traffic from that indicative of an impending attack. This can lead to problem of false positives, in which system mistakenly identifies legitimate traffic as some form of attack.

- A software system will simply alert administrator that suspicious activity has taken place. The human admin then makes decision whether or not to block traffic.
- If software automatically blocks any addresses it deems suspicious, you run risk of blocking out legitimate users.
- It should also be noted that nothing prevents offending user from moving to different machine to continue attack.
- This sort of approach should only be one part of an overall intrusion-detection strategy and not entire strategy.

2. Anomaly Detection:

- It involves actual software that works to detect intrusion attempts and then notify the administrator.
- The general process is simple, system looks for any abnormal behaviour. Any activity that does not match pattern of normal user access is noted and logged. The software compares observed activity against expected normal usages profiles.
- Profiles are usually developed for specific user, group of users, or applications. Any activity that does not match definition of normal behaviour is considered an anomaly and is logged.

- Sometimes above situation is referred to as “traceback” detection or “traceback” process. We are able to establish from where this packet was delivered.

The specific ways in which an anomaly is detected includes Threshold Monitoring, Resource Profiling, User/Group Work Profiling, and Executable Profiling. These are explained as following below.

3. Threshold Monitoring:

Threshold monitoring pre-sets acceptable behaviour levels and observes whether these levels are exceeded. This could include something as simple as finite number of failed login attempts or something as complex as monitoring the time user is connected and amount of data user downloads. Threshold monitoring provide definition of acceptable behaviour. Characterizing intrusive behaviour only by threshold limits can be somewhat challenging. It is often quite difficult to establish proper threshold values or proper time frames at which to check those threshold values. This can result in high rate of false positives in which system misidentifies normal usage as probable attack.

4. Resource Profiling:

It measures the system-wide use of resources and develops historic usage profile. Abnormal readings can be indicative of illicit activity underway. It might be difficult to interpret meaning of changes in overall system usages. An increase in usage might simply indicate something benign like an increased workflow rather than an attempt to breach security.

5. User/Group Work Profiling:

Here, the IDS maintains individual work profiles about user and groups. These users and groups are expected to obey these profiles. As the user changes his/her activities, his/her expected work profile is updated to reflect those changes. Some systems attempt to monitor interaction of short-term versus long-term profiles. The short-term profiles capture recent changing work patterns, whereas long-term profiles provide view of usages over an extended period of time. However, it can be difficult to profile an irregular or dynamic user base. Profiles that are defined too broadly enable any activity to pass review, whereas profiles that are defined too narrowly may inhibit user work.

6. Executable Profiling:

Executable profiling seeks to measure and monitor how programs use system resources, paying particular attention to those whose activity can always be traced to specific originating user. Example – system services usually cannot be traced to specific user launching them. Viruses, Trojan horses, worms, Tap-doors and other software attacks are addressed by profiling how system objects such as files and printers are normally used, not only by the user but also by other system subjects on the part of users. If the viruses inherit all of privileges of user executing software. Software is not limited by the principle of least privilege but to only those privileges needed to properly execute. This openness architecture permits viruses to covertly change and infect totally unrelated parts of system. Executable profiling enables IDS to identify activity that might indicate an attack. Once potential danger is identified, method of notifying administrator, such as by network message or email, is specific to individual IDS.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:
IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behaviour is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):**
   Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):**
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this

would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. **Hybrid Intrusion Detection System:**
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:**
   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. **Anomaly-based Method:**
   Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of **Intrusion Detection Systems (IDS)** because both IPS and IDS operate network traffic and system activities for malicious activity.

IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

Classification of Intrusion Prevention System (IPS):
Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analysing protocol activity.

2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analysing wireless networking protocols.

3. **Network behaviour analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

4. **Host-based intrusion prevention system (HIPS):**
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Comparison of Intrusion Prevention System (IPS) Technologies:

The Table below indicates various kinds of IPS Technologies:

IPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Only IDPS which can analyse the widest range of application protocols;
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS able to predict wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system (OS) activity; network, transport, and application TCP/IP layer activity	Individual host	Can analyse activity that was transferred in end-to-end encrypted communications

Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. **Stateful protocol analysis detection:**
   This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:
The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

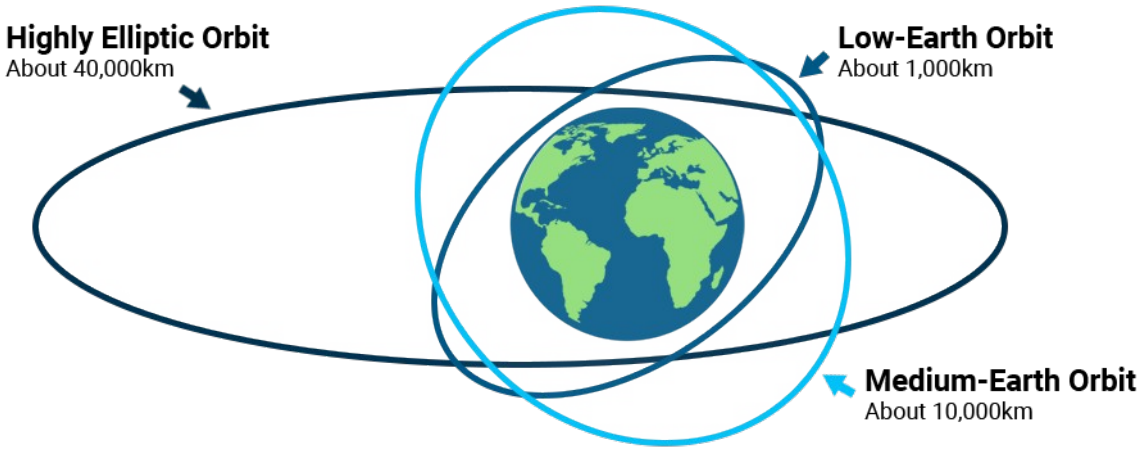
Thank You

Name – Saurabh Kumar	Class – MCA 3rd Yr (V Sem)
Roll No – 48	Subject – Mobile and Satellite Communication

Low Earth Orbit Satellite

Types of Satellites

- Geostationary/Geosynchronous Earth orbit satellite with a propagation delay of 250-280 ms.
- Medium Earth Orbit Satellites with a propagation dealy of 110-130 ms.
- Highly Elliptical Satellites with a variable propagation delay.
- Low Earth Orbit Satellite with a propagation delay of 20-25 ms.



Low Earth Orbit

A low Earth orbit (LEO) is an orbit around Earth with a period of 128 minutes or less and an eccentricity less than 0.25. Most of the artificial objects in outer space are in LEO, with an altitude never more than 2,000 km.

The mean orbital velocity needed to maintain a stable low Earth orbit is about 7.8 km/s, which translates to 28,000 km/h. However, this depends on the exact altitude of the orbit.

The pull of gravity in LEO is only slightly less than on the Earth's surface. This is because the distance to LEO from the Earth's surface is much less than the Earth's radius.

A low Earth orbit requires the lowest amount of energy for satellite placement. It provides high bandwidth and low communication latency. Satellites and space stations in LEO are more accessible for crew and servicing.

Since it requires less energy to place a satellite into a LEO, and a satellite there needs less powerful amplifiers for successful transmission, LEO is used for many communication applications, such as the Iridium phone system.

LEO satellites don't stay in fixed position relative to the surface. And a network of LEO satellites is necessary for LEO satellites to be useful.

Advantages

- It has least propagation delay (about 10ms) compare to other orbits due to closeness to the Earth. Due to lower latency, it can be used for realtime time critical applications.
- It eliminates need for bulky receiver equipments due to higher C/N signal ratio.
- It has flexible bandwidth
- It is also better for point to point communication.

Disadvantages

- A network of LEO satellites is needed, which can be costly.
- LEO satellites have to compensate for Doppler shifts caused by their relative movement.

Architecture of LEO

- Communication data passes through a satellite using a signal path known as a transponder.
- Satellites have 24-72 transponders. A single transponder is capable of handling up to 155 million bits of info per sec
- Today's communication satellites are an ideal medium for transmitting and receiving almost any kind of content – from simple to most complex contents.

Classes of LEO

- Little LEO
  - Operates under 1Ghz
  - Mostly used for low data rate messaging
  - Example: Orbcomm

- Big LEOs
  - Operates between 1 and 3 Ghz
  - Voice and limited data services
  - Example: Globalstar

- BroadBand LEOs
  - Provides communication similar to fiber optic networks
  - Example: SkyBridge

Applications of Satellite Networks

- Telecommunication
- Earth Observation
- Military Operations
- Natural Calamities
- Broadcasting Internet

Medium Earth Orbit Satellite.

(By: Priyanshu Gaur)

Satellite

A satellite is an object in space that orbits or circles around a bigger object. There are two kinds of satellites: natural (such as the moon orbiting the Earth) or artificial (such as the International Space Station orbiting the Earth).

We all know satellites are for wireless communication among earth's stations. They receive signals from one earth station and transmit them to other stations at larger distance from the remitting station.

Satellites are deployed into the space with all the necessary equipments and they then begins to orbit around the earth.

Types

So we have 3 types of satellites. Depending upon their distance from the earth we categorize them into 3 categories.

1. LEO means low earth orbit satellites.
2. MEO medium earth orbit satellites.
3. GEO seatationary earth orbit satellites.

Leo operates at from 160 to 2000 kms from earth. Like our ISS which is at 400 km from earth.

Geo operates above 35870 km.

The MEOs lies in between LEO and GEO range. They are also known as intermediate circular orbit (ICO) due to their position in between Leo and geo.

Orbital period

So every satellite orbits around the earth and their orbital period depends upon the distance from the earth. In case of MEO it can be anywhere from 2 hour to almost 24 hours. Or 23 hour 56 minutes and 4 secs.

With 24hours of orbital time period they are almost stationary with respect to an observer on the earth.

And at 20200 km the orbital time period becomes 12 hours which is used by the Global positioning system.

GPS overview

So GPS is a system of satellites which can determine your exact location on earth.

The Global Positioning System consists of 24 satellites, that circle the globe once every 12 hours, to provide worldwide position, time and velocity information. GPS makes it possible to precisely identify locations on the earth by measuring distance from the satellites. GPS allows you to record or create locations from places on the earth and help you navigate to and from those places.

Other Positioning systems

There are some other satellite positioning systems based on MEO

we have

- Russian GLONASS (altitude 19100 km)
- European Galileo (altitude 23222 km)
- Chinese BeiDou (altitude 21528 km)

And their respective distances

Also INIDIA now has its own positioning system operating at distance 36000 km.

Disadvantages

The disadvantages of MEO are as follows

1. Signal received from MEO are weaker than LEO.
2. They need tracking guided antennas.
3. MEO satellites are more expensive than Leo satellites.
4. Multiple satellites are required to cover a region continuously.
5. Increases orbital debris because of need of large number of satellites per system.

Advantages

Now for the advantages

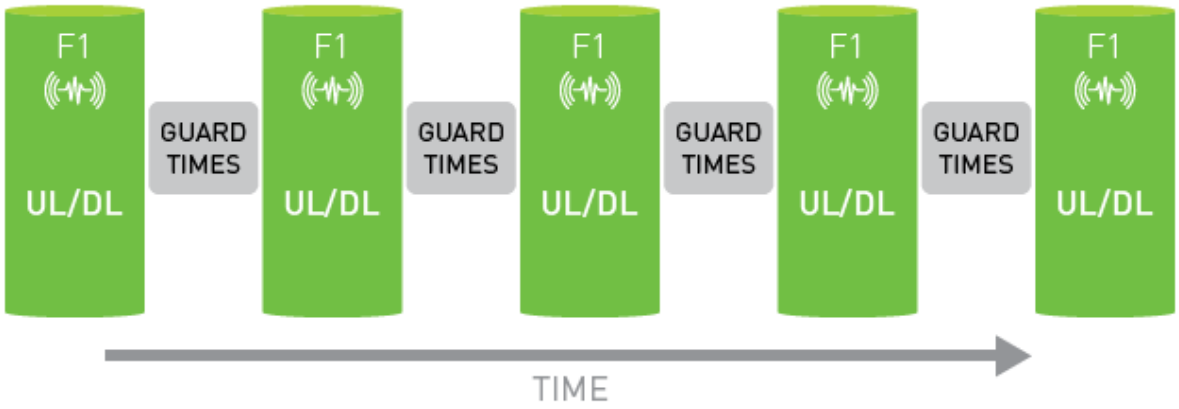
1. MEO satellites require less onboard fuel by launch vehicle.

2. Lesser number of satellites are required than LEO

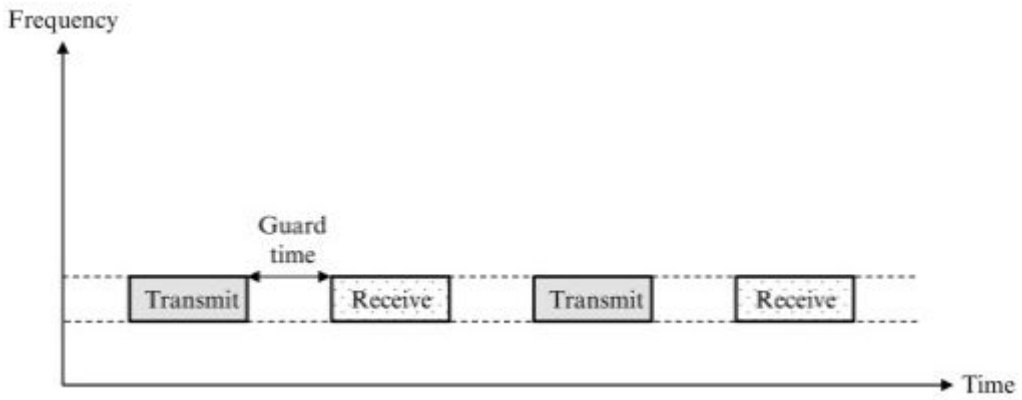
3. they can capture weaker signals than in GEO.

Time-division duplexing (TDD)

Time-division duplexing (TDD) is a method for emulating full-duplex communication over a half-duplex communication link. The transmitter and receiver both use the same frequency band but transmit and receive traffic at different times. TDD uses the same frequency band by assigning alternating time slots for transmit and receive operations. The information to be transmitted, whether it's voice, video, or computer data, is in a serial binary format. Each time slot may be 1 byte long or could be a frame of multiple bytes.



In time-division duplexing (TDD), time is used to separate the transmission and reception of the signals, rather than frequency (like in FDD), and thus a single frequency is assigned to a user for both directions. TDD provides a simultaneous bidirectional flow of information. Duplexers are therefore not required, and thus the cost of a TDD system is not very high, as the transmitter and receiver use the same components like filters and mixers.



TDD uses two-time slots, one for upstream (transmission) and the other for downstream (reception). A guard time between transmit and receive streams is allocated. Time-division duplexing facilitates concurrent send and receive by assigning transmitted signals in the one-time slot and received signals in another time slot. They share the same frequency channel.

TDD is used by Wi-Fi Networks and Some 4G/LTE Networks as well. Click here to see the LTE Bands that use TDD technology.

Advantages of TDD

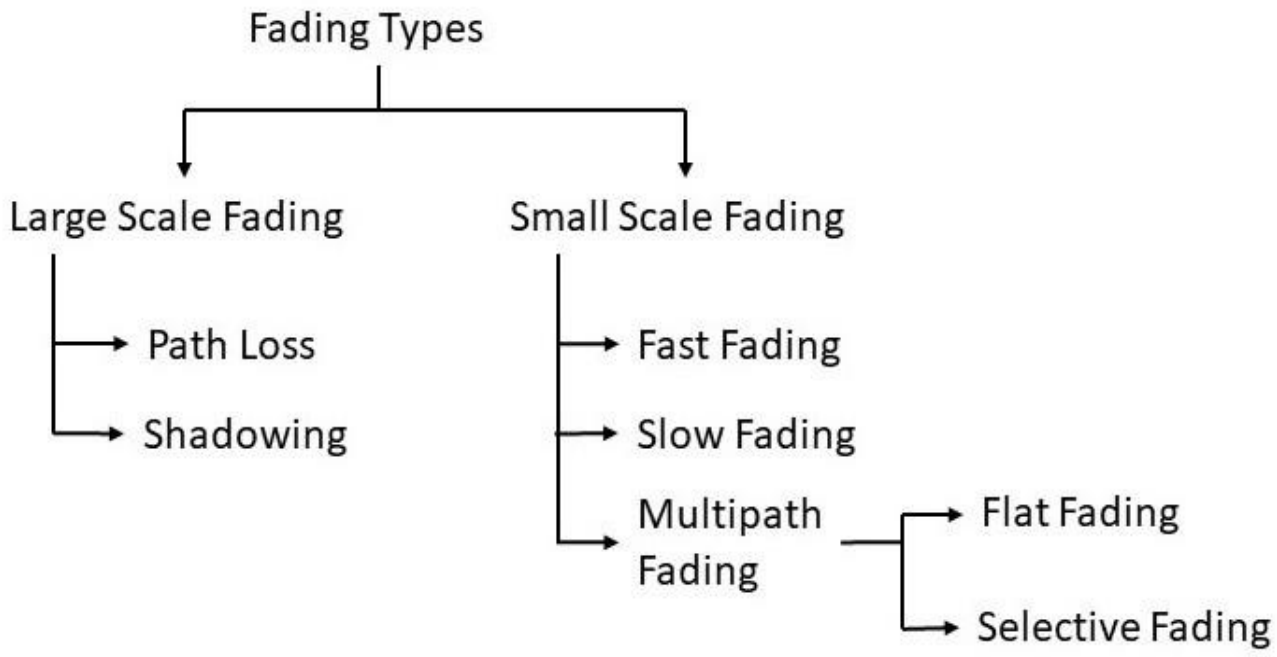
- It is more spectrum friendly, allowing the use of only a single frequency for operation and dramatically increasing spectrum utilization, especially in license-exempt or narrow-bandwidth frequency bands.
- It allows for the variable allocation of throughput between the transmit and receive directions, making it well suited to applications with asymmetric traffic requirements, such as video surveillance, broadcast, and Internet browsing.
- Radios can be tuned for operation anywhere in a band and can be used at either end of the link. As a consequence, only a single spare is required to serve both ends of a link.
- The cost of TDD Systems is lower as they can use the same components for Tx and Rx functions.

Disadvantages of TDD

- The switch from transmit to receive incurs a delay that causes traditional TDD systems to have greater inherent latency when compared to FDD systems.
- As TDD operates based on allocated time slots, it requires stringent phase/time synchronization to avoid interference between UL (Uplink) and DL (Downlink) transmissions.
- Multiple co-located radios can interfere with one another unless they are synchronized.
- Traditional TDD approaches yield poor TDM performance due to latency.
- For symmetric traffic (50:50), TDD is less spectrally efficient than FDD, due to the switching time between transmit and receive.

FADING

Fading is a phenomenon that occurs due to varying parameters and conditions of the channel during wireless propagation. To better understand and eliminate the adverse effects of fading, it is divided into various types. Let us take a look into them in detail.

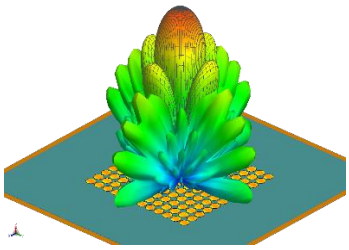


The figure above shows the different types of fading and the sub-categories. We have tried to elaborate on each type of fading below and provide information on how do they affect wave propagation.

1. Large Scale Fading: This refers to the attenuation of signal power due to obstacles between the transmitter and receiver. It also covers the attenuation and fluctuations of signal when the signal is transmitted over a long distance (usually in kilometres).

- **Path Loss:** It refers to the attenuation when a signal is transmitted over large distances. Wireless signals spread as they propagate through the medium and as the distance increases, the energy per unit area starts decreasing (Click here to try the Path Loss Calculator).This is a fundamental loss that is independent of the type of transmitter and medium. Although, we can minimize its effects by

increasing the capture area/dimension of the receiver. The figure below shows the radiation pattern and spread of the signal transmitted from the antenna.



- **Shadowing:** This refers to the loss in signal power due to the obstructions in the path of propagation. There are a few ways in which shadowing effects can minimize signal loss. One that is most effective, is to have a Line-Of-Sight propagation.

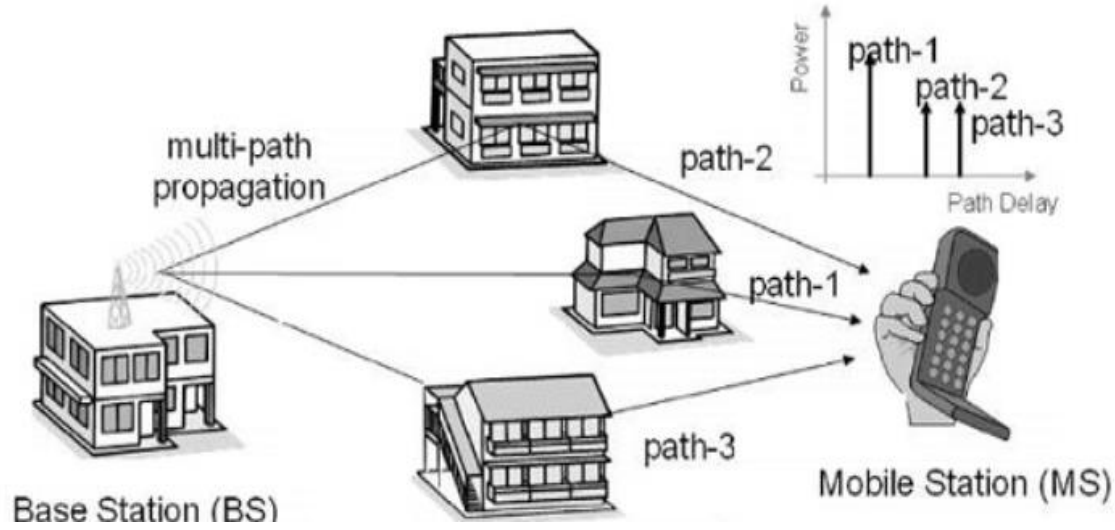
  Shadowing losses also depend on the frequency of the EM wave. As we know, EM Waves can penetrate through various surfaces but at the cost of loss in power i.e signal attenuation. The losses depend on the type of the surface and frequency of the signal. Generally, the penetration power of a signal is inversely proportional to the frequency of the signal.

2. Small Scale Fading: This refers to the fluctuations in signal strength and phase over short distance and small duration of time. It is also called Rayleigh Fading. Small Scale Fading affects almost all forms of wireless communication and overcoming them is a necessity to increase efficiency and decrease error.

- **Fast Fading:** It occurs mainly due to reflections for surfaces and movement of transmitter or receiver. High doppler spread is observed in the fast fading with Doppler bandwidth comparable to or greater than the bandwidth of the signal and the channel variations are as fast or faster than the signal variations. It causes linear distortions in the shape of the baseband signal and creates Inter Symbol Interference (ISI). One way to remove ISI is adaptive equalization.
- **Slow Fading:** It occurs mainly due to shadowing where large buildings or geographical structures obstruct the LOS. Low doppler spread is observed in Slow Fading with the doppler bandwidth being smaller compared to the bandwidth of the signal and the channel variations are slow relative to the signal variations. It results in reduction of SNR which can be overcome using error correction techniques and receiver diversity techniques.
- **Multipath Fading:** It occurs when a signal reaches the receiver from various path i.e. when multipath propagation takes place. Multipath fading can affect all ranges of frequencies starting from low frequency to microwave and beyond.

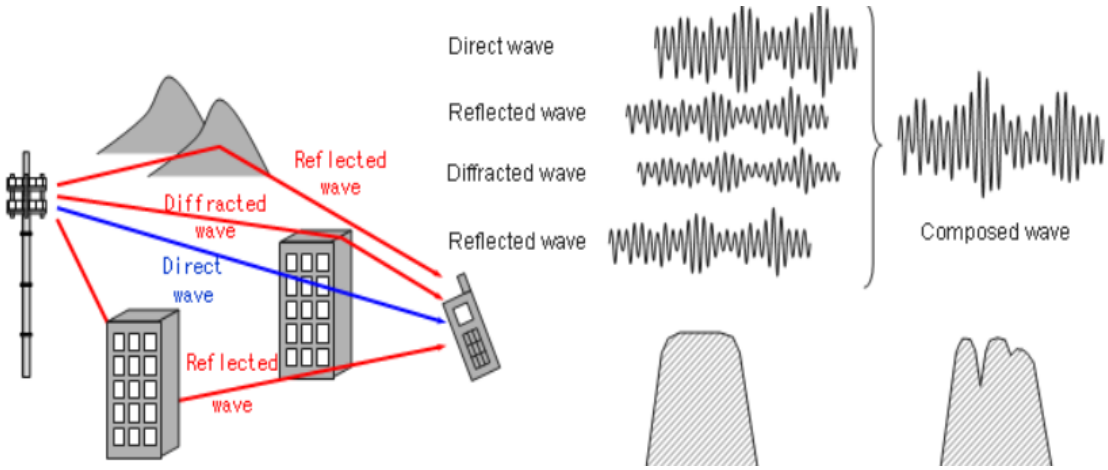
Multipath Fading

- In wireless telecommunications, multipath is the propagation phenomenon that results in radio signals' reaching the receiving antenna by two or more paths. Causes of multipath include atmospheric ducting, ionospheric reflection and refraction, and reflection from terrestrial objects, such as mountains and buildings.
- The effects of multipath include constructive and destructive interference, and phase shifting of the signal. This causes Rayleigh fading, named after Lord Rayleigh. The standard statistical model of this gives a distribution known as the Rayleigh distribution.
- Rayleigh fading with a strong line of sight content is said to have a Rician distribution, or to be Rician fading.
- In facsimile and television transmission, multipath causes jitter and ghosting, seen as a faded duplicate image to the right of the main image. Ghosts occur when transmissions bounce off a mountain or other large object, while also arriving at the antenna by a shorter, direct route, with the receiver picking up two signals separated by a delay. In radar processing, multipath causes ghost targets to appear, deceiving the radar receiver. These ghosts are particularly bothersome since they move and behave like the normal targets (which they echo), and so the receiver has difficulty in isolating the correct target echo. These problems can be overcome by incorporating a ground map of the radar's surroundings and eliminating all echoes which appear to originate below ground or above a certain height. In digital radio communications (such as GSM) multipath can cause errors and affect the quality of communications. The errors are due to Intersymbol interference (ISI). Equalisers are often used to correct the ISI. Alternatively, techniques such as orthogonal frequency division modulation and Rake receivers may be used.



Causes of Multipath Fading

It includes atmospheric reflection and refraction, and reflection from water bodies and terrestrial objects such as mountains and buildings.



It affects both the amplitude and the phase of the signal causing phase distortions and ISI. Multipath fading can affect signal transmission in two ways:

- **Flat Fading:** In flat fading, all frequency components get affected almost equally. Flat multipath fading causes the amplitude to fluctuate over a period of time.
- **Selective Fading:** Selective Fading or Selective Frequency Fading refers to multipath fading when the selected frequency component of the signal is affected. It means selected frequencies will have increased error and attenuation as compared to other frequency components of the same signal. This can be overcome by techniques such as OFDM which spreads the data across the frequency components of the signal to reduce data loss.

TDMA

• Time division multiple access (TDMA) is digital transmission technology that allows a number of users to access a single radio-frequency (RF) channel without interference by allocating unique time slots to each user within each channel.
• The TDMA digital transmission scheme multiplexes three signals over a single channel.
- The current TDMA standard for cellular divides a single channel into six time slots, with each signal using two slots, providing a 3 to 1 gain in capacity over advanced mobile-phone service (AMPS). Each caller is assigned a specific time slot for transmission.

How TDMA works?

TDMA relies upon the fact that the audio signal has been digitized; that is, divided into a number of milliseconds-long packets.

It allocates a single frequency channel for a short time and then moves to another channel.

The digital samples from a single transmitter occupy different time slots in several bands at the same time.

• The access technique used in TDMA has three users sharing a 30-kHz carrier frequency. •

The reason for choosing TDMA for all these standards was that it enables some vital features for system operation in an advanced cellular or PCS environment.

Advantages of TDMA

In addition to increasing the efficiency of transmission, TDMA offers a number of other advantages over standard cellular technologies. First and foremost, it can be easily adapted to the

transmission of data as well as voice communication.
TDMA offers the ability to carry data rates of 64 kbps to 120 Mbps (expandable in multiples of 64 kbps).
• It is the most cost effective technology for upgrading analog to digital.
• It provides the user with extended battery life and talk time.
• Dual band 800/1900 MHz.

Disadvantages of TDMA

•One of the disadvantages of TDMA is that each user has a predefined time slot. However, users roaming

from one cell to another are not allotted a time slot.
Another problem with TDMA is that it is subjected to multipath distortion.
A signal coming from a tower to a handset might come from any one of several directions. It might have bounced off several different buildings before arriving

Point Coordination Function

Point Coordination Function (PCF)

Point coordination function (PCF) is an optional technique used to prevent collisions in IEEE 802.11-based WLAN standard including Wi-Fi. It is a medium access control (MAC) sublayer technique used in areas where carrier-sense multiple access with collision avoidance (CSMA/CA) is used.

PCF is used additionally along with the mandatory distributed coordination function (DCF). It is used in centralised control system, and is present in the access point (AP) of the wireless network. An AP is generally a wireless router that coordinates network communication.

Features of PCF

- It is an optional function that resides on the top of the mandatory DCF. Both PCF and DCF operate simultaneously.
- It provides channel access to the stations using poll and response method thus eliminating the need of contention.
- The polling is done by the point co-ordinator (PC) that resides in central access point (AP).
- The station waits for Point Inter–Frame Space (PISF) before transmission. PISF is typically smaller than DIFS (Distributed Inter-Frame Space) as used in DCF.
- PC polls in a round – robin method to provide access to the stations in the wireless network.
- AP issues a special control frame called beacon frame to initiate and repeat polling.

PCF Interframe Space

PCF Interframe Space (PIFS) is one of the interframe space used in IEEE 802.11 based Wireless LANs. PCF enabled access point wait for PIFS duration rather than DIFS to occupy the wireless medium. PIFS duration is less than DIFS and greater than SIFS (DIFS > PIFS > SIFS). Hence AP always has more priority to access the medium.

PIFS duration can be calculated as follows:

PIFS = SIFS + Slot time

Standard	Slot time (µs)	PIFS (µs)
IEEE 802.11-1997 (FHSS)	50	78
IEEE 802.11-1997 (DSSS)	20	30
IEEE 802.11b	20	30
IEEE 802.11a	9	25
IEEE 802.11g	9 or 20	19 or 30
IEEE 802.11n (2.4 GHz)	9 or 20	19 or 30
IEEE 802.11n (5 GHz)	9	25
IEEE 802.11ac	9	25

Technique

Step 1 − PC sends a beacon frame after waiting for PIFS. The beacon frame reaches every station in the wireless network.

Step 2 − If AP has data for a particular station, say station X, it sends the data and a grant to station X.

Step 3 − When station X gets the grant from the AP, if it has a data frame for AP, it transmits data and acknowledgement (ACK) to the AP.

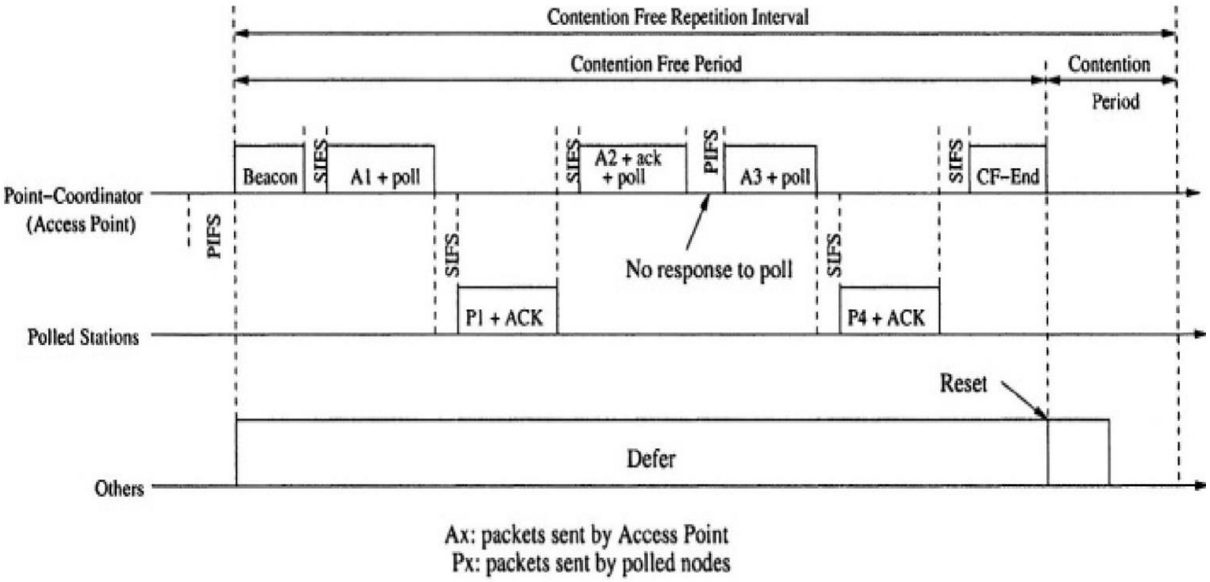
Step 4 − On receiving data from station X, the AP sends an ACK to it.

Step 5 − The AP then sends goes to the next station, say station Y. If AP has data for Y, it sends data and grant to Y, otherwise it sends only grant to Y.

Step 6 − On receiving grant from AP, station Y transmits its data (if any) to AP.

Step 7 − This process continues for all the stations in the poll.

Step 8 − At the end of granting access to all the stations, the AP sends an ACK to the last station. It then notifies all stations that this is the end of polling.



Ax: packets sent by Access Point
Px: packets sent by polled nodes

Thank You

Modulation Techniques
And
BandWidth Estimation

Shivam Dixit
52
MCA(3rd Year)

- **What is Modulation?**

  The process by which data/information is converted into electrical/digital signals for transferring that signal over a medium is called modulation.

- **Types Of Modulation Techniques**

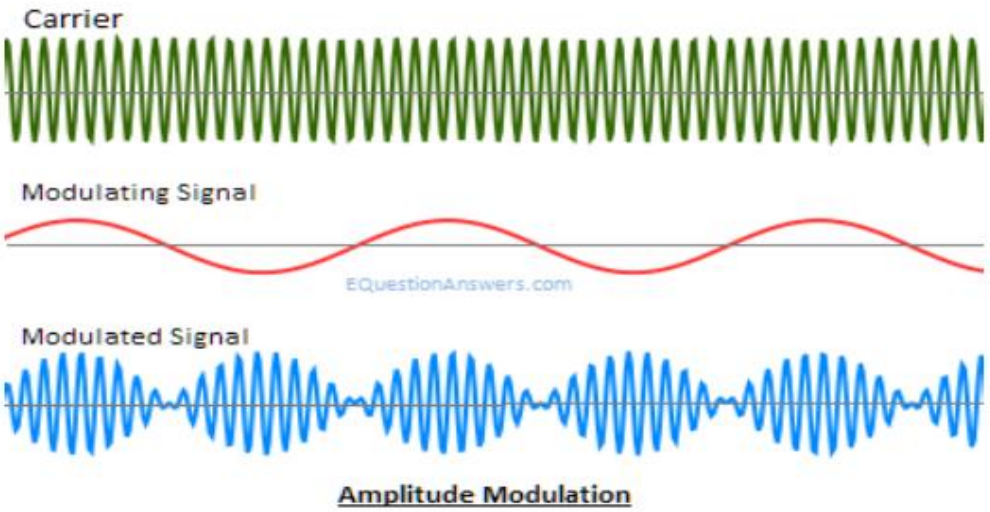
  - Analog Modulation
    - *Amplitude Modulation*
    - *Frequency modulation*

  - Digital Modulation

- **Analog Modulation**

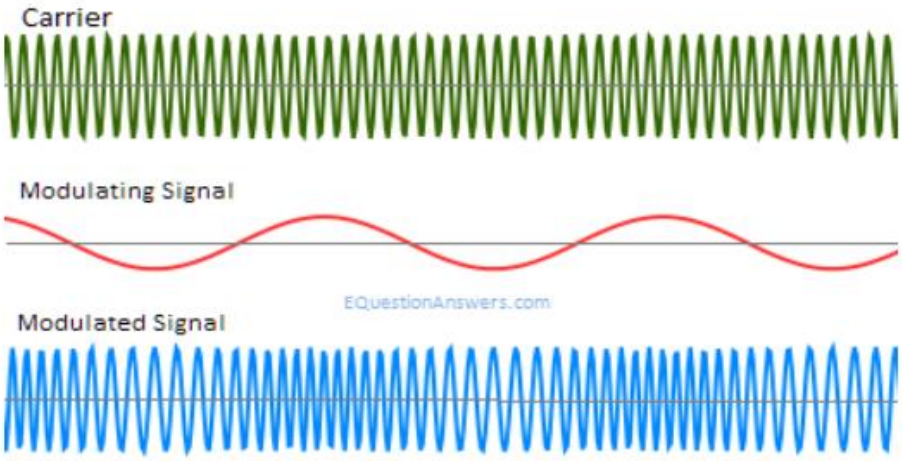
  It is a process of transferring analog low frequency signal over a high frequency carrier signal.In other words, you can say that "Analog Modulation is a technique which is used in analog data signals transmission into digital signals."

  - **Amplitude Modulation:** The process of superimposing the message signal over carrier wave to change the amplitude is called amplitude modulation.



Amplitude Modulation

- **Frequency Modulation:** The process of super imposing the message signal over carrier wave t change the frequency is called frequency modulation.



Frequency Modulation

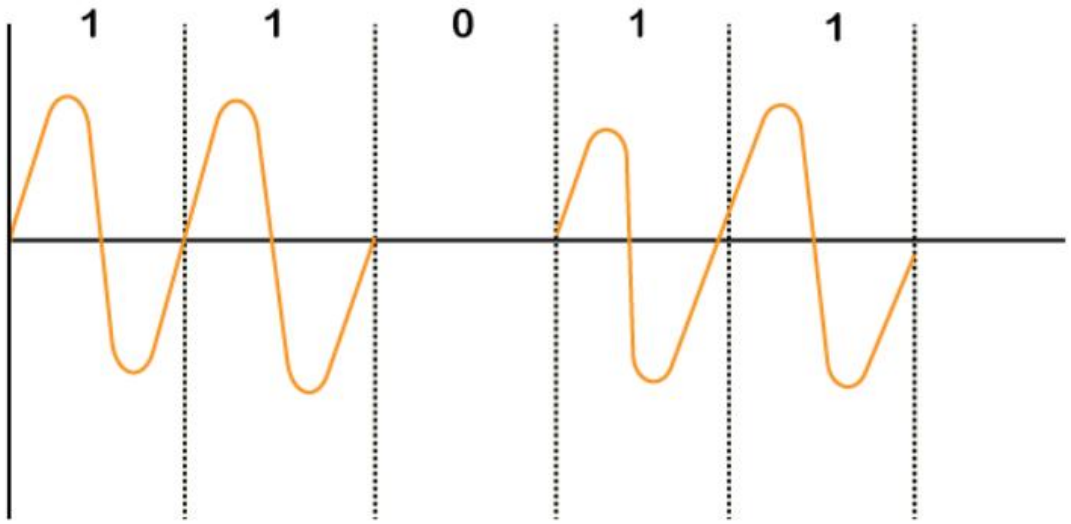
- **Digital Modulation**

a) Digital Modulation is a technique in which digital signals/data can be converted into analog signals.

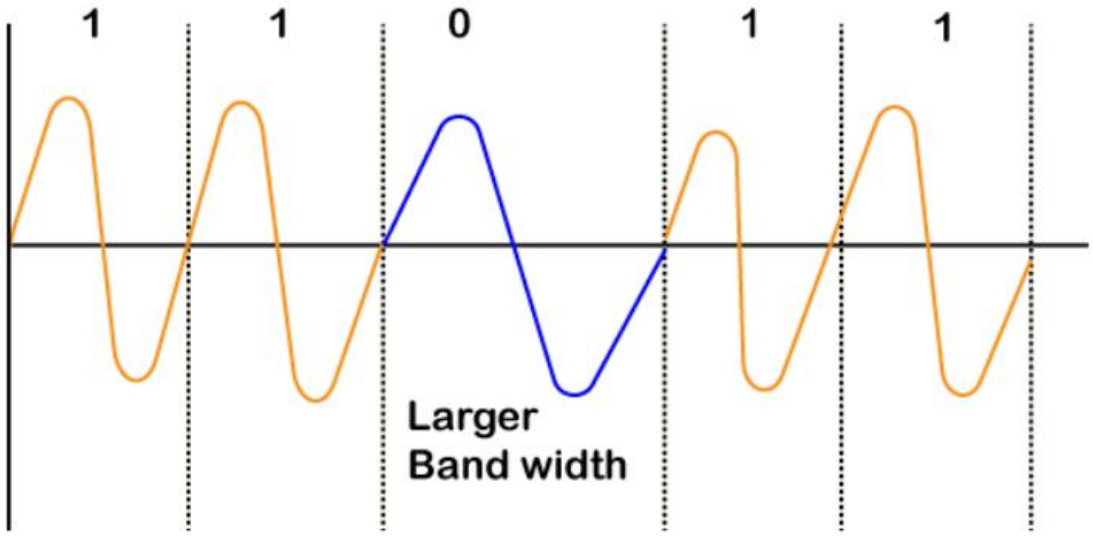
b) The carrier wave is keyed or switched on and off to create pulses such that the signal is modulated.

c) The types of digital modulation are based on the type of signal and application used such as Amplitude Shift Keying, Frequency Shift Keying..

- **Amplitude Shift Keying:**As the name suggests, in Amplitude Shift Key the amplitude is represented by "1," and if the amplitude does not exist, it is represented by "0".



- **Frequency Shift Keying:**In Frequency Shift Key or FSK Modulation, different notations f1 and f2 are used for different frequencies. Here, f1 is used to represent bit "1," and f2 represents bit "0".



- **Bandwidth Estimation**

In a packet network, the terms bandwidth often characterize the amount of data that the network can transfer per unit of time.

Bandwidth estimation is of interest to users wishing to optimize end-to-end transport performance, overlay network routing, and peer-to-peer file distribution.

Existing bandwidth estimation tools measure one or more of three related metrics: capacity, available bandwidth, and bulk transfer capacity.

Mobile Satellite Notes for SDMA

If we talk about a common medium, where multiple signals are present at the same time. It is very difficult to provide **interference free** transmission.

Interference: When two or more signals have the same frequency & they are present at the same time in the same medium, they will overlap with each other. This will change their signal strength abruptly.

So, how can we provide interference free transmission?

Solution is **multiple access technique.**

The main idea is to provide the interconnection of multiple users which are present in the common medium at the same time in the interference free environment.

We can use channelization.

Channelization is to divide common physical medium, so that we can provide interference free environment for multiple users.

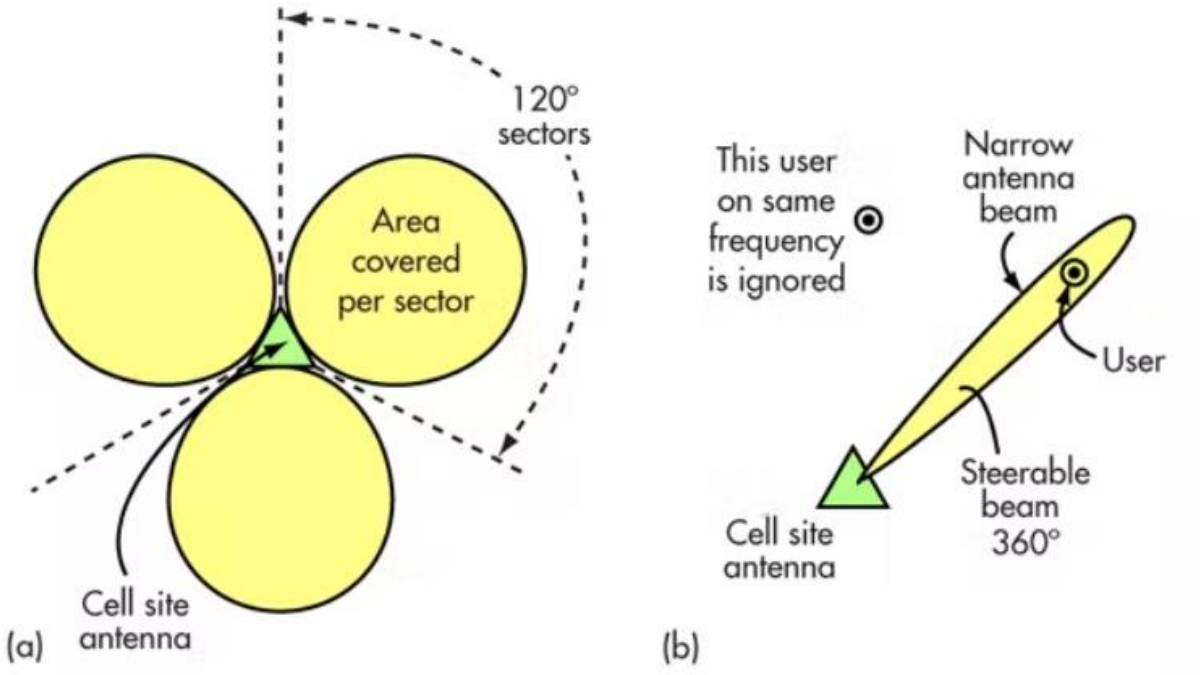
Types of channelization.

- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)
- **SDMA (Space Division Multiple Access)**

SDMA (Space Division Multiple Access)

- No two user should transmit in the same space.
- It depends on the user position information and provides users access to the communication channel based on their spatial locations.
- A single channel may be used simultaneously, if the users are spaced far enough from one another to avoid interference. This is known as frequency reuse.
- Traditionally cellular base stations radiate power in all directions, because they have no information about where the mobile device is located. This wastes power and causes interference to adjacent cells, as well as making it harder to distinguish weaker incoming signals from among the noise and interference.

- By using smart antenna technology to track the spatial location of mobile devices, the radiation pattern of the base station can be adjusted to optimize both transmission & reception for each user device.
- By rapidly adjusting the phase of signals from several antennas, the base signals from several antennas, the base station can effectively steer a beam or spot of RF power to or from each user.



6. SDMA separates users on shared frequencies by isolating them with directional antennas. Most cell sites have three antenna arrays to separate their coverage into isolated 120° sectors (a). Adaptive arrays use beamforming to pinpoint desired users while ignoring any others on the same frequency (b).

Features of SDMA

- It is completely free from interference.
- Can control the medium access for a wireless network.
- Controlled radiated energy for each user in space.
- All user can communicate at the same time using the same channel.
- It can track the moving user.
- It is never used in isolation.

Advantages of SDMA

- Increases the capacity and speed of the system.
- Increases transmission quality by focusing the signal into narrow transmission beams.
- Free from interference.
- All users can communicate at the same time using the same channel.
- Two different signals can use the same frequency.
- It minimizes system cost.
- Increases the range.

Disadvantages of SDMA

- Very expensive
- Complicated to construct and design.
- Perfect adaptive antenna system: infinitely large antenna needed.

VSAT Satellites

- **Hard to reach areas**
- **Reliability : reliable satellite transmission of data between an unlimited number of geographically dispersed sites.**
- **Time to deploy (4-6 months vs. 1-2 weeks)**
- **Cost (If distance is more than 500 km then the VSAT solution is more cost-effective as compared to the optical fiber.)**

Introduction To VSAT

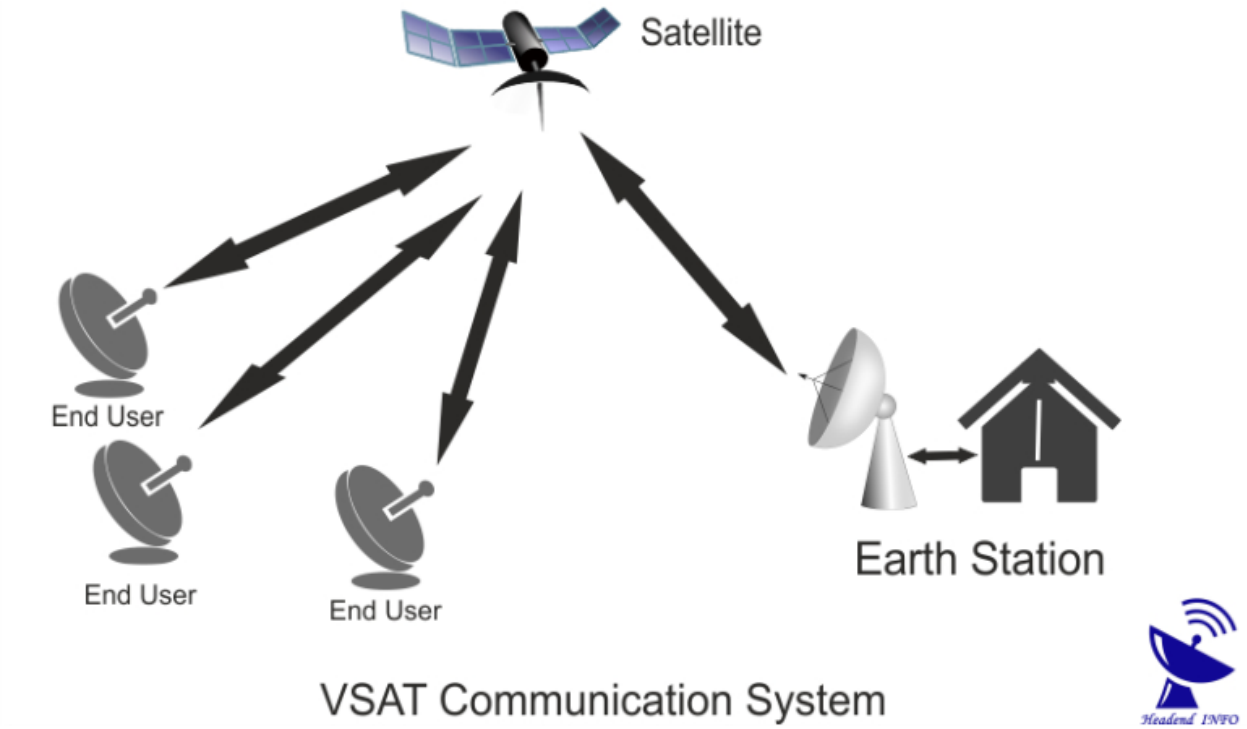
A Very Small Aperture Terminal (VSAT) is a device known as a small private earth station - that is used to transmit & receive data signal through a satellite. VSAT stands for Very Small Aperture Terminal and refers to receive/transmit terminals installed at dispersed sites connecting to a central hub via satellite using small diameter antenna dishes (0.6 to 3.8 meter). VSAT is used for both broadcast & interactive applications of effective data, voice and video transfer.

- A Very Small Aperture Terminal (VSAT), is a two-way satellite ground station with a dish antenna that is smaller than 3 meters.

- VSATs access satellites to relay data from small remote earth stations (terminals) to other terminals (in mesh configurations) or master earth station "hubs" (in star configurations).
- Underlying objective of VSAT Systems: bring the service directly to the end-user

Why VSAT?

The dish is small, easily transportable and installation lead-time is much shorter if compared to terrestrial links. VSAT network allows rapid, low-cost network re-configuration and expansion to meet new or unexpected business requirements. Cost effective transmission and network operations are made possible by use of the Ex-C band satellite frequency and frequency times division multiple access (FTDMA), Frequency division multiple access (FDMA) or Time division multiple access (TDMA) transmission techniques.



- Data rates in VSATs ranges from 4 Kbps to 16 Mbps.
- It accesses satellites in geosynchronous orbits or geostationary orbits.

- A VSAT has a dish antenna with diameters between 75 cm to 1 m, which is very small in comparison with 10 m diameter of a standard GEO antenna

TYPES OF SATELLITES

According to orbit position satellites are of mainly three types:

- LEO(Low Earth Orbit satellite)
- MEO(Medium Earth Orbit satellite)
- GEO(Geosynchronous Equatorial Orbit satellite)

Need of VSAT

- Hard to reach areas
- Reliability : reliable satellite transmission of data between an unlimited number of geographically dispersed sites.
- Time to deploy (4-6 months vs. 1-2 weeks)
- Cost (If distance is more than 500 km then the VSAT solution is more cost-effective as compared to the optical fiber.)

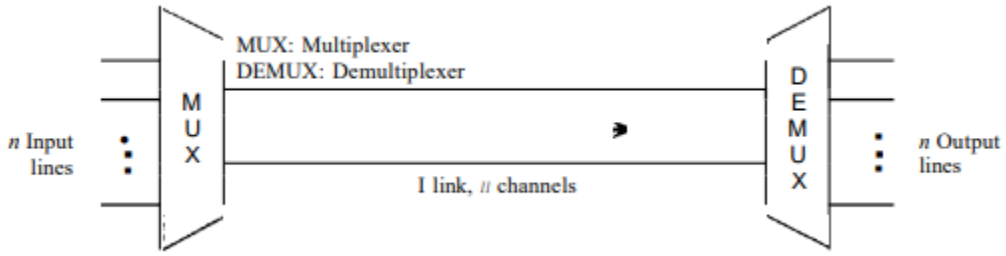
Applications Of VSAT

- In narrowband data − e.g. point – of – sale transactions using debit cards or credit cards, RFID data
- In broadband data − e.g. Internet access to remote locations, VoIP
- Mobile communications
- Maritime communications

Wavelength Division Multiple Access

MULTIPLE ACCESS TECHNIQUES

Multiple access techniques are used to allow a large number of mobile users to share the allocated spectrum in the most efficient manner.



Need of Multiple access

- As the spectrum is limited, so the sharing is required to increase the capacity of cell or over a geographical area by allowing the available bandwidth to be used at the same time by different users.
- And this must be done in a way such that the quality of service doesn't degrade within the existing users.

Wavelength Division Multiple Access

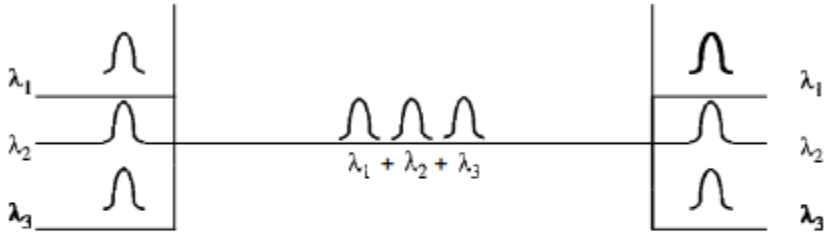
To allow multiple transmission at the same time, the spectrum is divided into channels (wavelength bands)

WDMA is a technique that uses Wavelength division multiplexing and some protocols by which two or more than two terminals connected to the same

transmission medium can transmit over it and to share its capacity over wavelength.

Wavelength Division Multiplexing

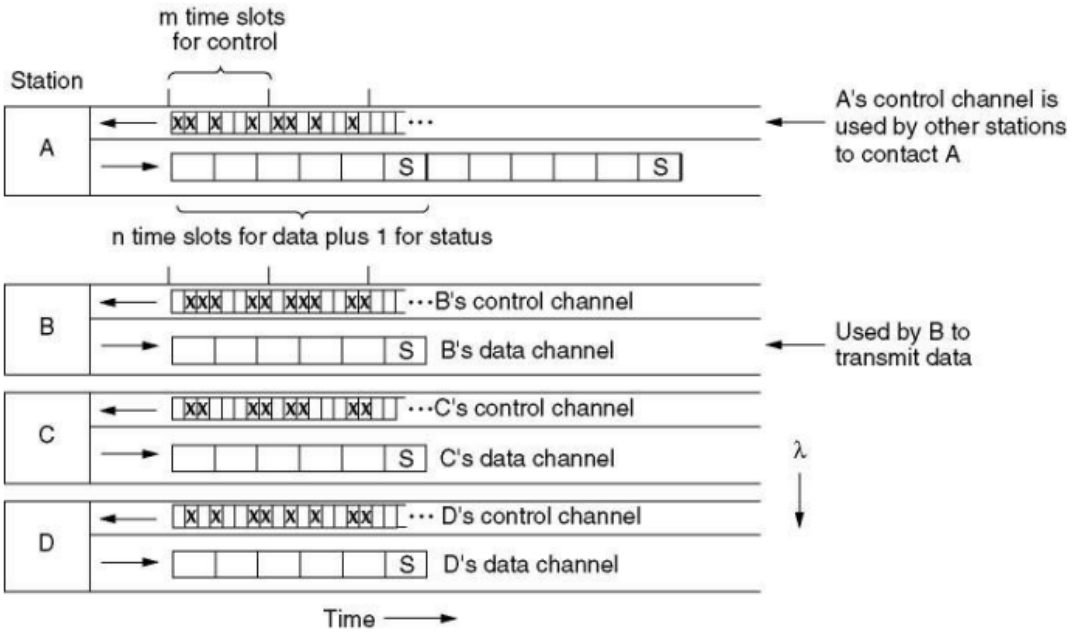
Wavelength division multiplexing (WDM) is a technique of multiplexing multiple optical carrier signals through a single optical fiber channel by varying the wavelengths of laser lights. WDM allows communication in both the directions in the fiber cable.



WDM is an analog multiplexing technique to combine optical signals.

Protocol for WDMA

In this protocol, WDMA, each station is assigned two channels. A narrow channel is provided as a control channel to signal the station, and a wide channel is provided so the station can output data frames.



Each channel is divided into groups of time slots. On both channels, the sequence of slots repeats endlessly, with slot 0 being marked in a special way so latecomers can detect it. All channels are synchronized by a single global clock.

Ref-

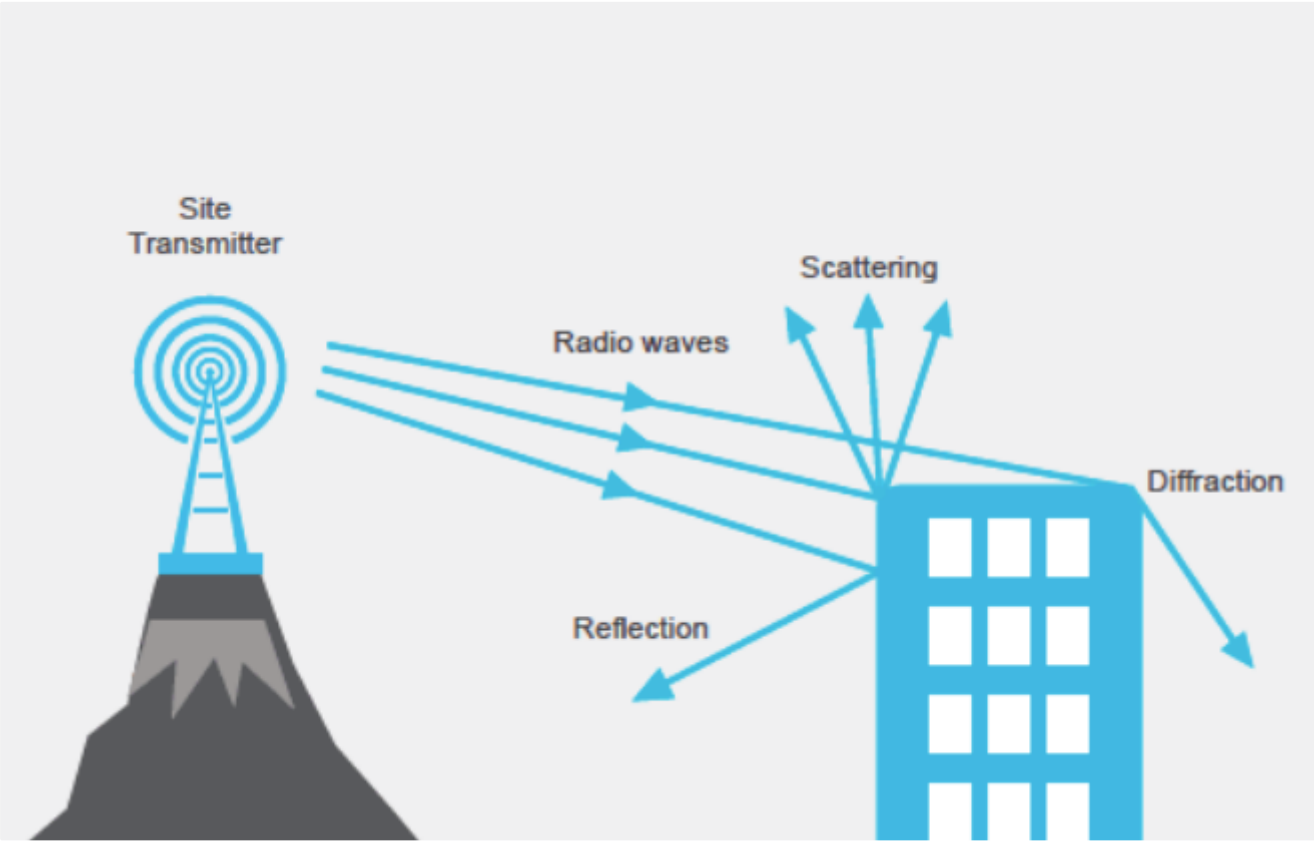
https://www.techopedia.com/definition/8469/multiple-access

http://android.eng.ankara.edu.tr/wp-content/uploads/sites/656/2017/09/Week_7.pdf

Wireless Propagation Characteristics

Basic Propagation Mechanisms

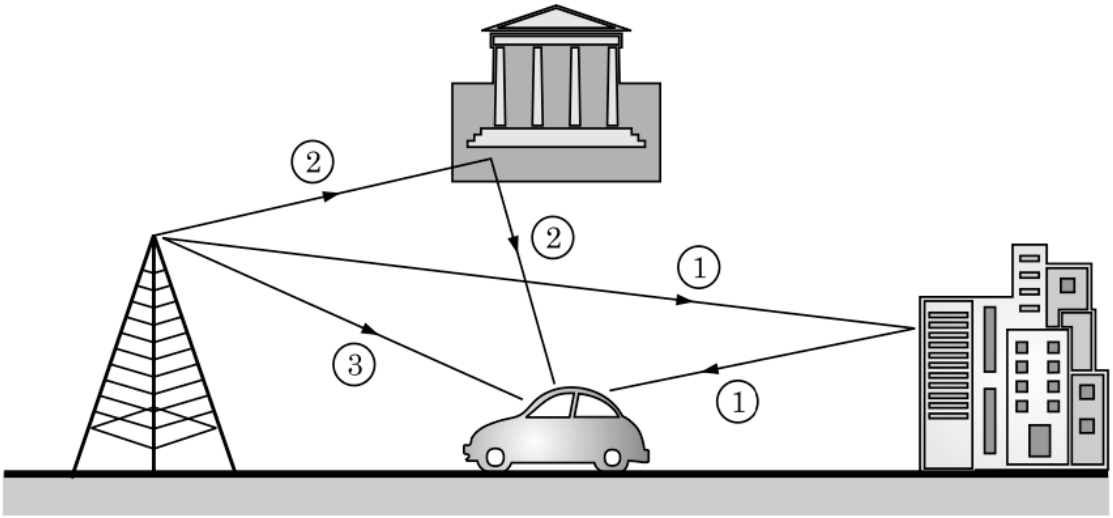
- **Reflection** — when an EM wave encounters a surface or obstacle and bounces back to its source. This causes loss of signal.
- **Diffraction** — Corners and sharp surfaces cause an EM wave just like the one thrown from a router to split into secondary smaller waves.
- **Scattering** — When the signal encounters a surface it dissipates into multiple reflected signals.



Multipath Propagation

- In multipath propagation, multiple signal paths are established between the base station and the user terminal (mobile phone).

- The fading due to multipath propagation is known as **Multipath fading** or Rayleigh fading.
- These indirect signals can add to or subtract from the direct signal arriving at the antenna.



Interference

Multipath interference is a phenomenon in the physics of waves whereby a wave from a source travels to a detector via two or more paths and the two (or more) components of the wave interfere constructively or destructively. Multipath interference is a common cause of "ghosting" in analog television broadcasts and of fading of radio waves.

In this illustration, an object (in this case an aircraft) pollutes the system by adding a second path. The signal arrives at receiver (RX) by means of two different paths which have different lengths. The main path is the direct path, while the second is due to a reflection from the plane.

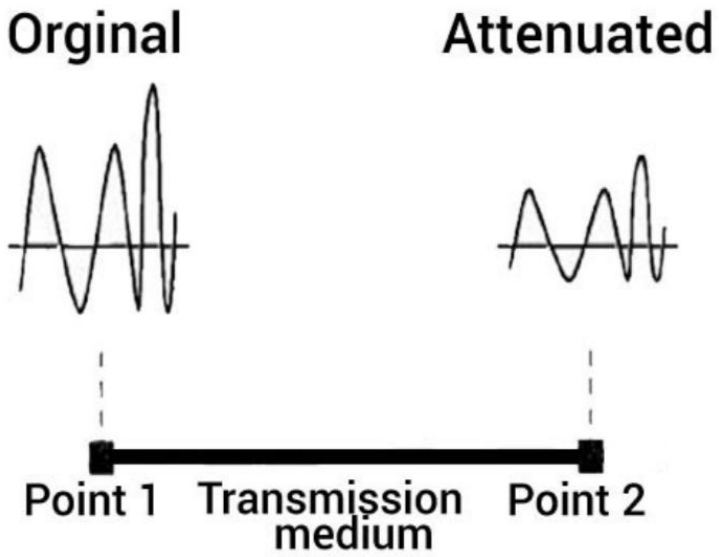
> 💡 The condition necessary is that the components of the wave remain coherent throughout the whole extent of their travel.

The interference will arise owing to the two (or more) components of the wave having, in general, travelled a different length (as measured by optical path length – geometric length and refraction (differing optical speed)), and thus arriving at the detector out of phase with each other.

The signal due to indirect paths interferes with the required signal in amplitude as well as phase which is called multipath fading.

Attenuation

Attenuation refers to the loss of signal strength with distance over any transmission medium.



Causes

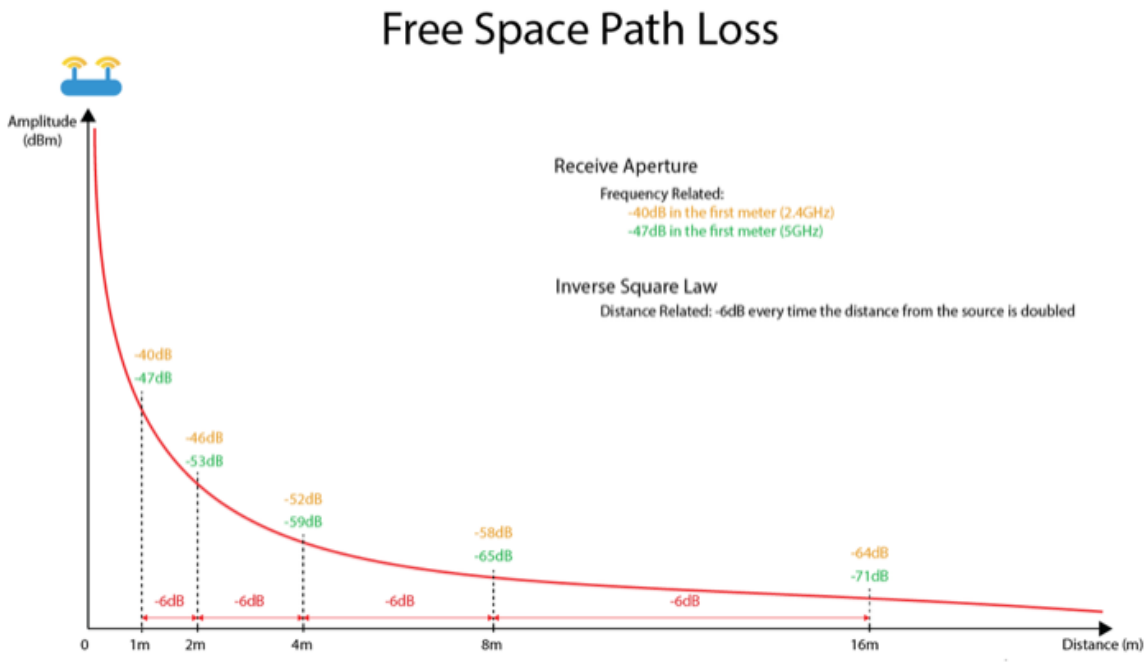
Other than distance, there are a few causes of signal attenuation:

- **Long cabling** – Over a long distance, transmitted signals slowly lose strength.
- **Wire size** – Thin wires experience more attenuation than thicker wires because they are more vulnerable to external interferences.
- **Noise** – Adjacent wires can cause electromagnetic interferences. The higher the noise, the higher the attenuation.
- **Defective connectors and conductors** – Poorly installed connectors and conductors lead to attenuation.

Path Loss

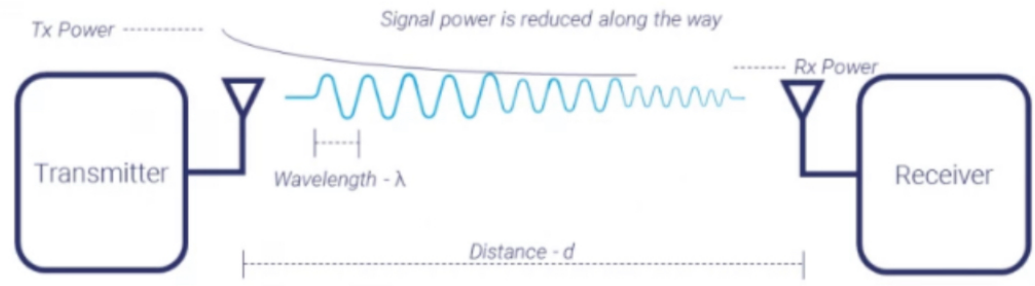
- Path Loss refers to the loss or attenuation a propagating electromagnetic signal or wave encounters along its path from the transmitter to the receiver.
- Also expressed as the ratio of transmitted power to received power

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



In decibels, path loss can be expressed as

$$L_{\text{dB}} = 10 \log \frac{P_t}{P_r} = 20 \log \left(\frac{4\pi d}{\lambda}\right)$$



Causes

Path loss normally includes *propagation losses* caused by the natural expansion of the radio wave front in free space (which usually takes the shape of an ever-increasing sphere), *absorption losses* (sometimes called penetration losses), when the signal passes through media not transparent to electromagnetic waves, *diffraction losses* when part of the radio-wave front is obstructed by an opaque obstacle, and losses caused by other phenomena.

The signal radiated by a transmitter may also travel along many and different paths to a receiver simultaneously; this effect is called multipath. Multipath waves combine at the receiver antenna, resulting in a received signal that may vary widely, depending on the distribution of the intensity and relative propagation time of the waves and bandwidth of the transmitted signal. The total power of interfering waves in a Rayleigh fading scenario varies quickly as a function of space (which is known as *small scale fading*). Small-scale fading refers to the rapid changes in radio signal amplitude in a short period of time or distance of travel.

💡 Multipath waves combine at the receiver antenna, resulting in a received signal that may vary widely, depending on the distribution of the intensity and relative propagation time of the waves and bandwidth of the transmitted signal.

Fading

Fading refers to the fluctuations in signal strength when received at the receiver. These are basically unwanted variations introduced at the time when the signal propagates from an end to another by taking multiple paths. Fading can be classified into two types:

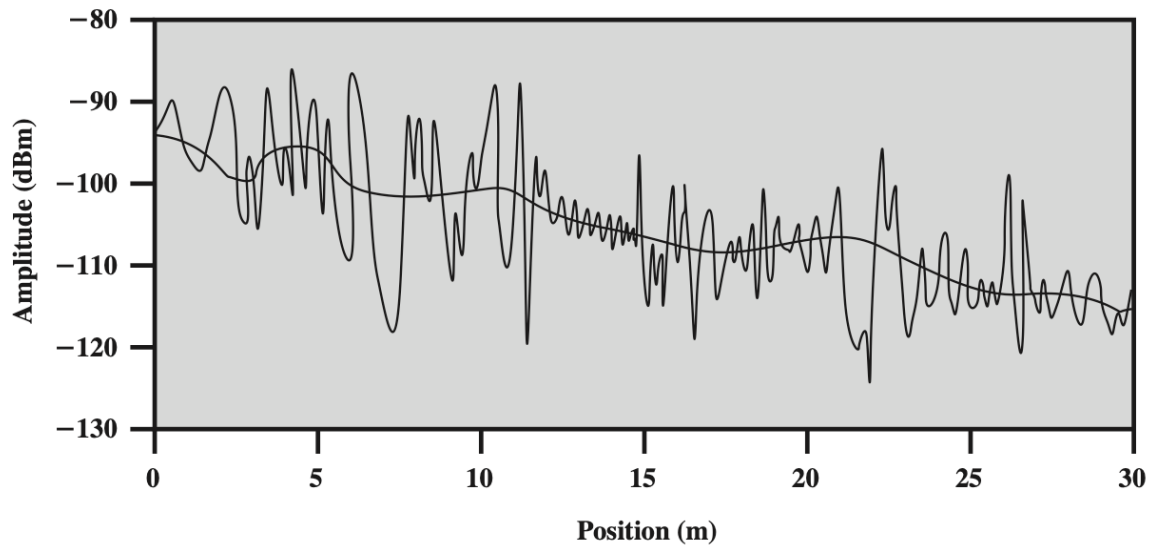
1. Fast Fading
2. Slow Fading

Fast Fading

- Fast Fading refers to the rapid fluctuations in the amplitude, phase or multi path delays of the received signals, due to the interference between multiple versions of the same transmitted signal arriving at the receiver at slightly different times.
- The multiple signal paths may sometimes add constructively or sometimes destructively at the receiver causing a variation in the power level of the received signal.

Slow Fading

- The name Slow Fading itself implies that the signal fades away slowly.
- Slow fading occurs when objects that partially absorb the transmission lie between the transmitter and receiver.
- Slow fading is also referred to as **shadow fading** since the objects that cause the fade, which may be large buildings or other structures, block the direct transmission path from the transmitter to the receiver.



Selective fading

It is also known as frequency selective fading. Basically when waves propagate through different paths by being reflected from various man-made entities then the different frequencies get affected to different degrees.

This will lead to cause variation in the amplitude and phase of the signals to a different extent while propagating in the channel.

It is to be noted that even if the path length through which the signal is propagating is same, then also the signals will possess different wavelengths. This causes variation in the phase of the signal across the overall bandwidth.

Selective fading can occur over a quite large range of frequencies. Suppose signals are utilizing ground wave propagation and sky wave propagation, then in such case the phase of the signals will change with time as the two are using two different medium of propagation.

Thus combinely when the signals are received at the receiving antenna then there will be changes in the received signal from the actually transmitted one.

So, as this type of fading is frequency selective, thus at the time of propagation, even adjacent parts of the signal fade independently even if their frequency of separation is small.

Hence we can say, this causes **severe distortion** of the modulated signal.

As it severely affects high-frequency signals thus is more dangerous in case of sky wave propagation. The amplitude modulated signals are generally more prone to such distortions rather than SSB signals.

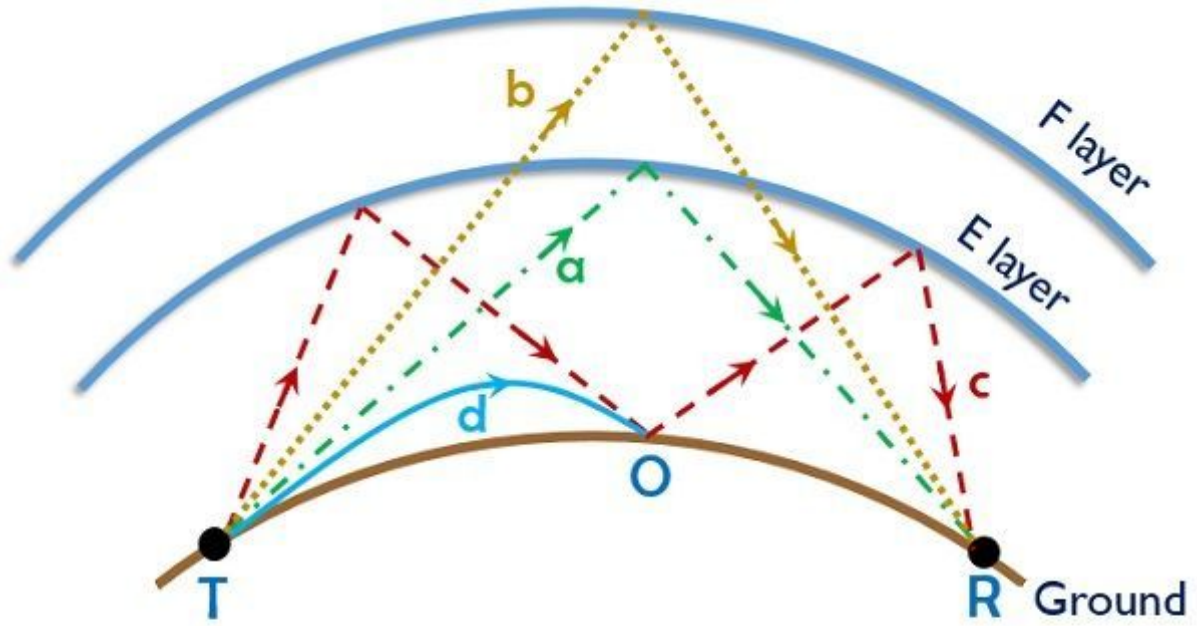
Thus one can use SSB systems to reduce selective fading.

Interference fading

Interference fading is also a result of the multipath propagation of signals transmitted from the antenna. It occurs when waves interfere at the channel while propagating from an end to another.

Suppose a signal is propagated through sky wave propagation, then the waves travel by getting reflected from the upper and lower regions of the ionosphere. Sometimes the waves propagate through single or multiple hops also, in case of low-frequency signals. Thereby leading to cause interference of signals in the channel.

The figure below represents interference fading caused due to the propagation of rays through multiple paths:



Interference fading due to various rays in the atmosphere

Electronics Desk

- Here ray ‘a’ is reflected from E layer,
- ray ‘b’ is reflected from F layer,
- ray ‘c’ is multihop propagation and
- ray ‘d’ is groundwave.

It is noteworthy here that sometimes it occurs even due to variation in the ionization density. Basically with the variation in path length, there is random variation in the phase and thus amplitude changes continually thus cause interference of waves.

Absorption fading

We know that when the signal propagates from an end to another then there are losses that are introduced by the transmission medium. Generally, when the signal is propagated through any medium, then the medium possesses some amount of signal absorption.

However, the amount of signal being absorbed by the medium is not constant as this depends on various factors. Thus it will be wrong to say that every transmitted signal suffers an equal amount of absorption while propagating through the same medium.

So, due to the absorption of the signal by the transmission medium, the strength of the signal varies and this deteriorates the received signal.

Polarization fading

Polarization fading is the result of variation in the polarization of the waves reaching the surface of the earth.

In sky wave propagation when wave reflects back to the surface of earth then its polarization changes. The change in polarization of the reflected wave is the result of the superposition of other waves (ordinary and extraordinary) with opposite polarization that are having different amplitudes and phases.

This leads to cause change in polarization of the wave continually with the antenna. Hence the amplitude of the signal received at the receiver also varies.

Thus is known as **polarization fading**.

Skip fading

Here the name itself is indicating that this type of fading is associated with skip distance of radio wave propagation.

It generally occurs near the skip distance region. This type of fading is an outcome of variation in the height and ionization density of the ionospheric region.

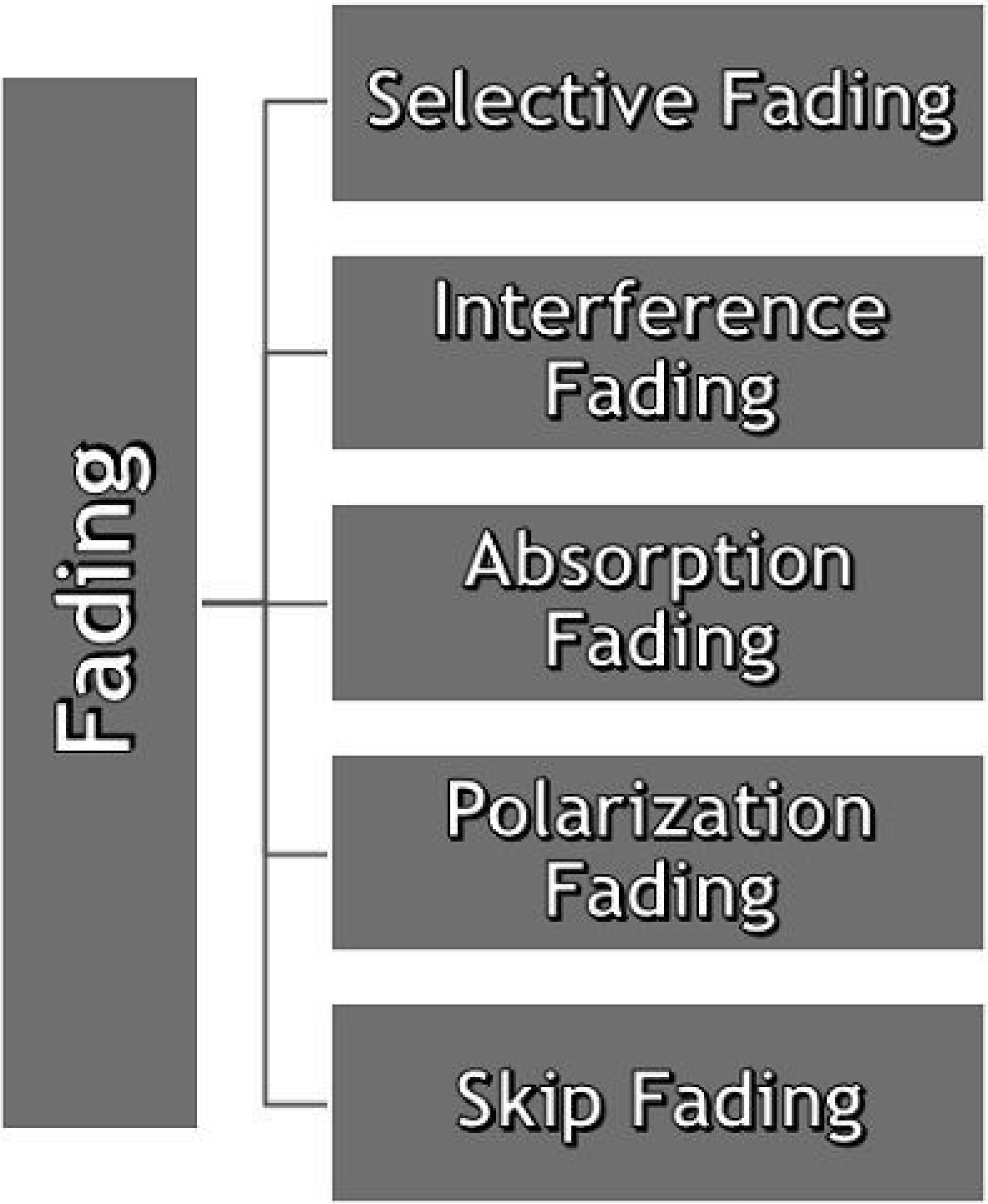
We are aware of the fact that skip distance is the region between transmitting and receiving point where the signal is received after getting reflected from the ionosphere.

So, the variation in the ionization density will undoubtedly alter the skip zone. This variation can be a point either in or out of the skip zone.

Now the question arises on how to deal with fading?

So, generally, a method commonly used to reduce fading is to use automatic voltage control at the receiving section. But this does not act as a complete solution because it does not show usefulness when the signal level reduces below the noise level.

As in such a case, the amplification will not be of any use. Also, this method does not support selective fading. Thus a diversity reception system is used to reduce the fading of the signal.



Electronics Desk