Lecture – 01

Security Models

No Security: In this simplest case, the approach could be a decision to implement no security at all.

Security through Obscurity: A system is secure simply because nobody knows about its existence and content.

Host Security: The security of each host is enforced individually.

Network Security: Host security is tough to achieve as an organizations grow and become more diverse, in this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is efficient and scalable model.

Security Management Practices

Goodsecuritymanagementpractices always talkofthesecuritypolicybeingin-place.

A good security policy generally takes care of four key aspects.

1. **Affordability** – How much money and efforts does the security implementation cost.
2. **Functionality** – What is the mechanism of providing security?
3. **Cultural Issues** – Does the policy gel well with the people's expectations, working style and beliefs?
4. **Legality** – Does the policy meet the legal requirement?

Additionally, a good security policy should also take care of:

1. Explanation of the policy to all the concerned.
2. Outline every one responsibilities.
3. Use simple language in all communications.
4. Accountability should be established.

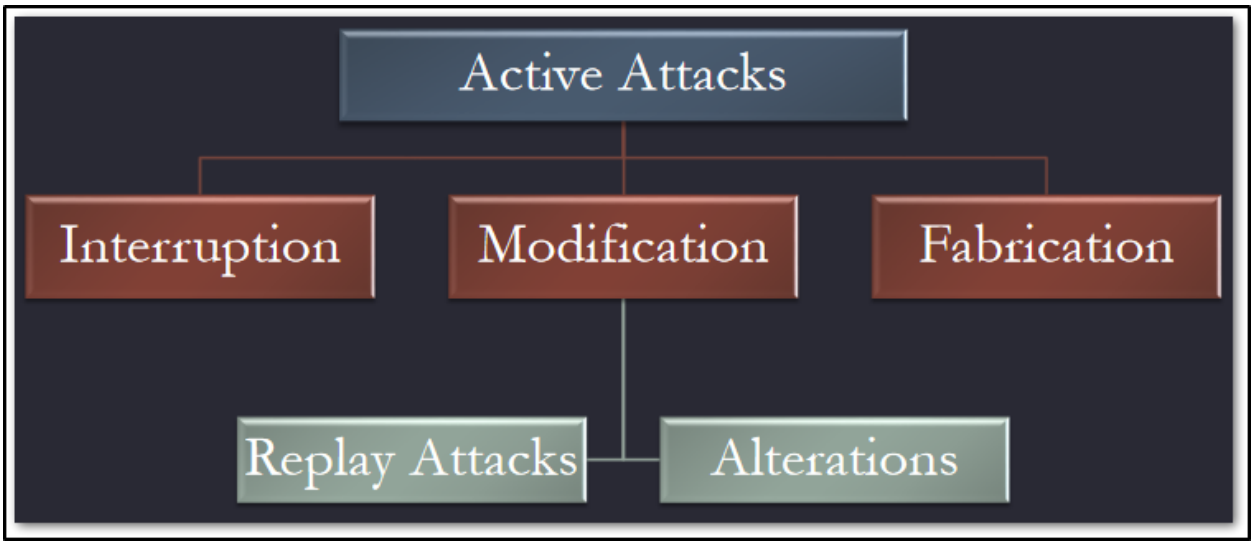
Principles of Security

1. **Confidentiality**: Information is only accessed by authorized individuals.
2. **Integrity**: Information is only modified by authorized individuals.
3. **Authentication:** Verify that the subject is someone that it claims.
4. **Non-Repudiation:** Sender cannot deny that he/she did not send message.
5. **Availability:** Information is available to authorized individuals when required.
6. **Access Control:** Who is authorized to access what information on what level.

Types of Attacks

Passiveattacks, do not involve any modifications to the content of an original message.

Active attacks, the contents of the original message are modified in some way.



Computer Virus, Worms & Trojans

Virus: A *computer virus* is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code.

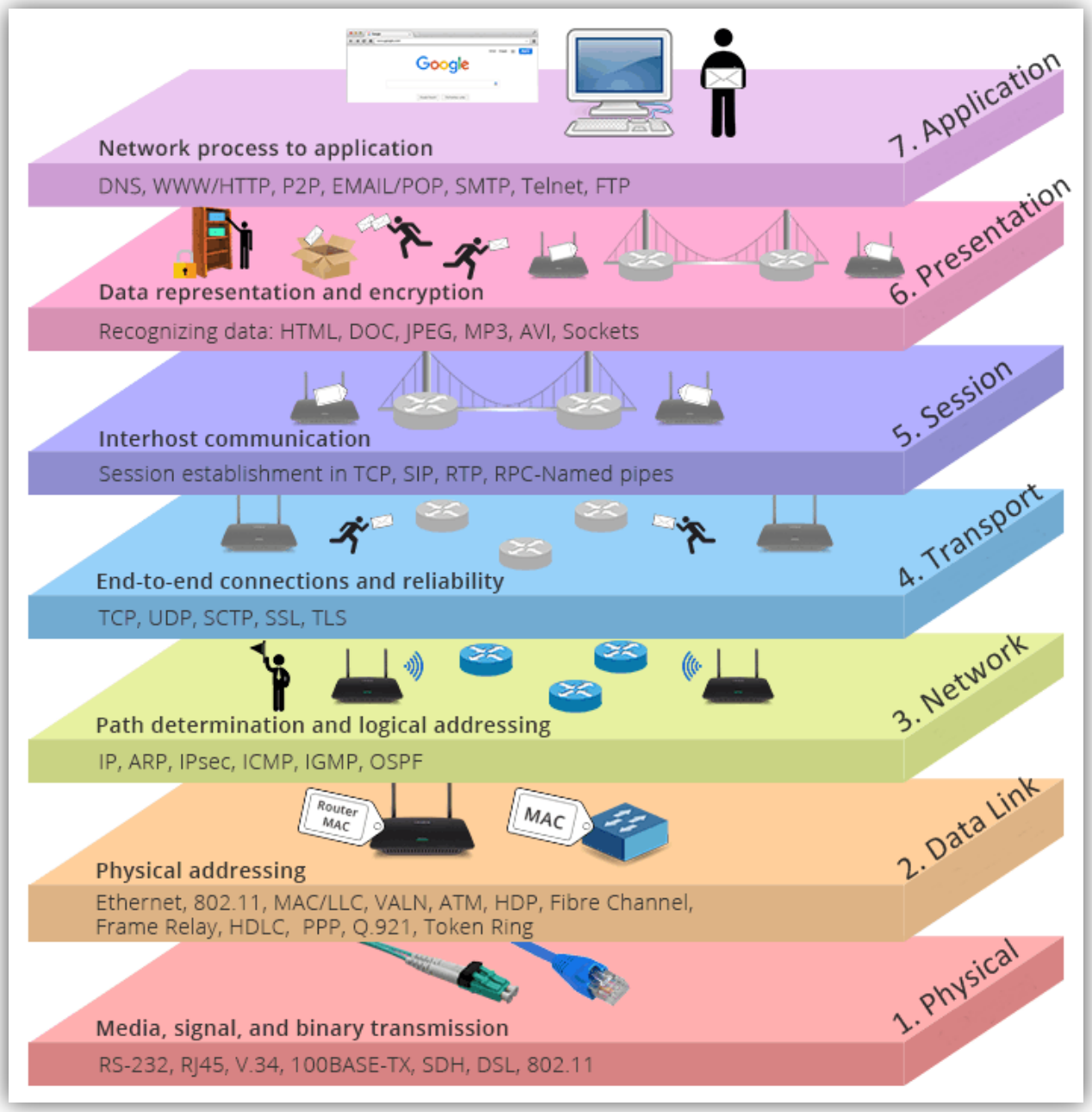
Worm: A *computer worm* is a type of malware that spreads copies of itself from computer to computer. It can replicate itself without any human interaction.

Trojan: A*Trojan horse* or *Trojan* is a type of malware that is often disguised as legitimate software.

Lecture – 02

OSI Layer Model

Open System Interconnection (OSI) is a network communication model that establishes standards of communication. It comprises of seven layers and each layer is responsible to treat data of its above or below layer.



Layer	Description
1: Physical	• It converts bits into frames and vice versa • Devices: Repeater, Hubs, Multiplexer • **Data Unit**: Bits
2: Data Link	• It performs error handling and coverts frames into packets and vice versa. • Further divided into two layers: LLC – for flow control & error handling and MAC – for access to physical media • Devices: Switch, Bridge • **Data Unit**: Frames
3: Network	• It performs switching, routing and packets forming operations. • Devices: Router, ATM Switch • **Data Unit**: Packets
4: Transport	• It performs flow control, QoS, end-to-end data transmission, and conversion of segments into packets and vice versa. • **Data Unit**: Segments
5: Session	• It is used to establish sessions between systems, dialogue control & synchronization. • **Data Unit**: Data
6: Presentation	• It is used for data encoding, compression, and encryption. • **Data Unit**: Data
7: Application	• It supports software applications to access network. • **Data Unit**: Data

Advantages of OSI

- Network communication is broken into smaller, more manageable parts.
- Allows different types of network hardware and software to communicate with each other.
- All layers are independent and changes does not affect other layers.
- Easier to understand network communication.

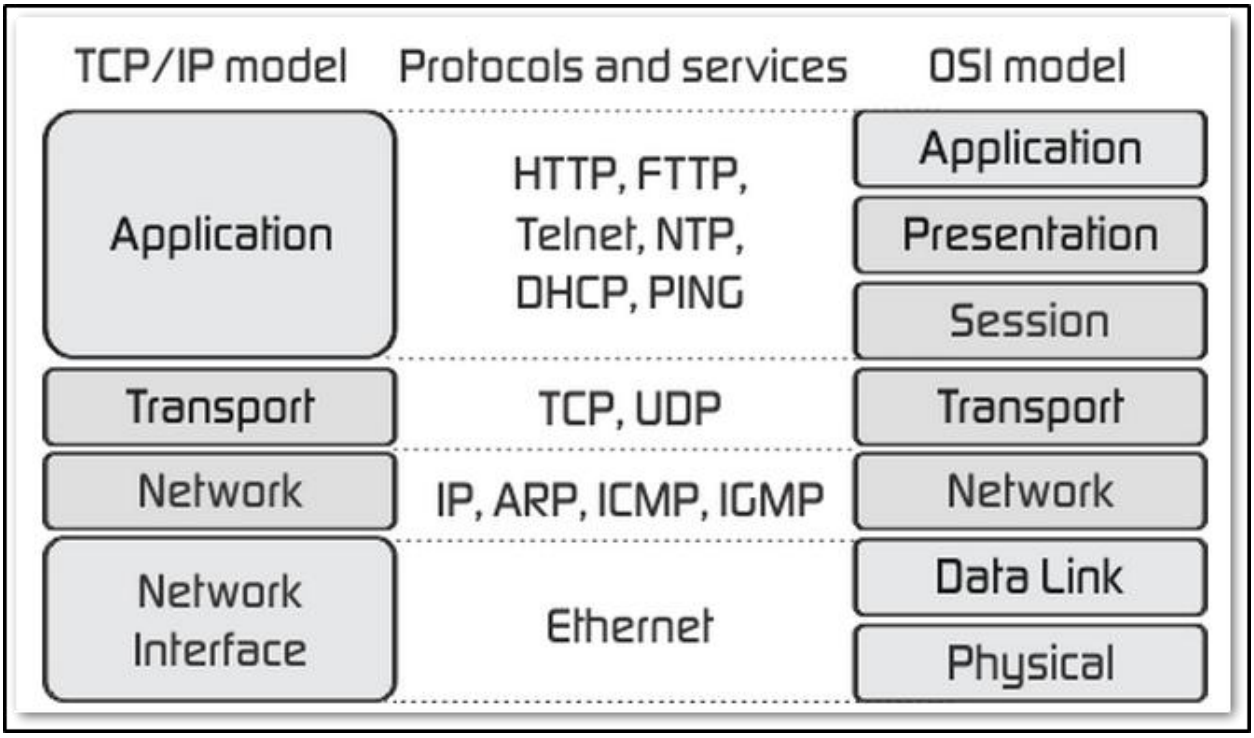
TCP/IP Model

TCP

- Guarantees end to end delivery of data segments
- Connection-oriented
- Reliable process to process communication service

IP

- Data sent over internet from source to destination.
- IP is connection less (packets independent, different routes, out of order).



OSI VS TCP/TIP

Similarities

Both have layers

Both have application, transport, and network layers

Both assume packets are switched. This means that individual packets may take different paths to reach the same destination.

Differences

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears simpler because it has fewer layers.
- TCP/IP protocols are the standards around which the Internet developed

Lecture – 03: Satellite Communication

Why Satellite Communication?

The purpose of communications satellites is to relay the signal around the curve of the Earth allowing communication between widely separated geographical points.

Satellite

Communication Satellite at its basic level is a repeater that receives, amplifies, and forwards signals.

Satellite Stations

There are two earth stations in a simple satellite communication link.

- **Transmitting Earth Station** used to transmit signals to satellite.
- **Receiving Earth Station** used to receive signals from satellite.

Links

There are two links in satellite communication and are called **uplink**&**downlink**.

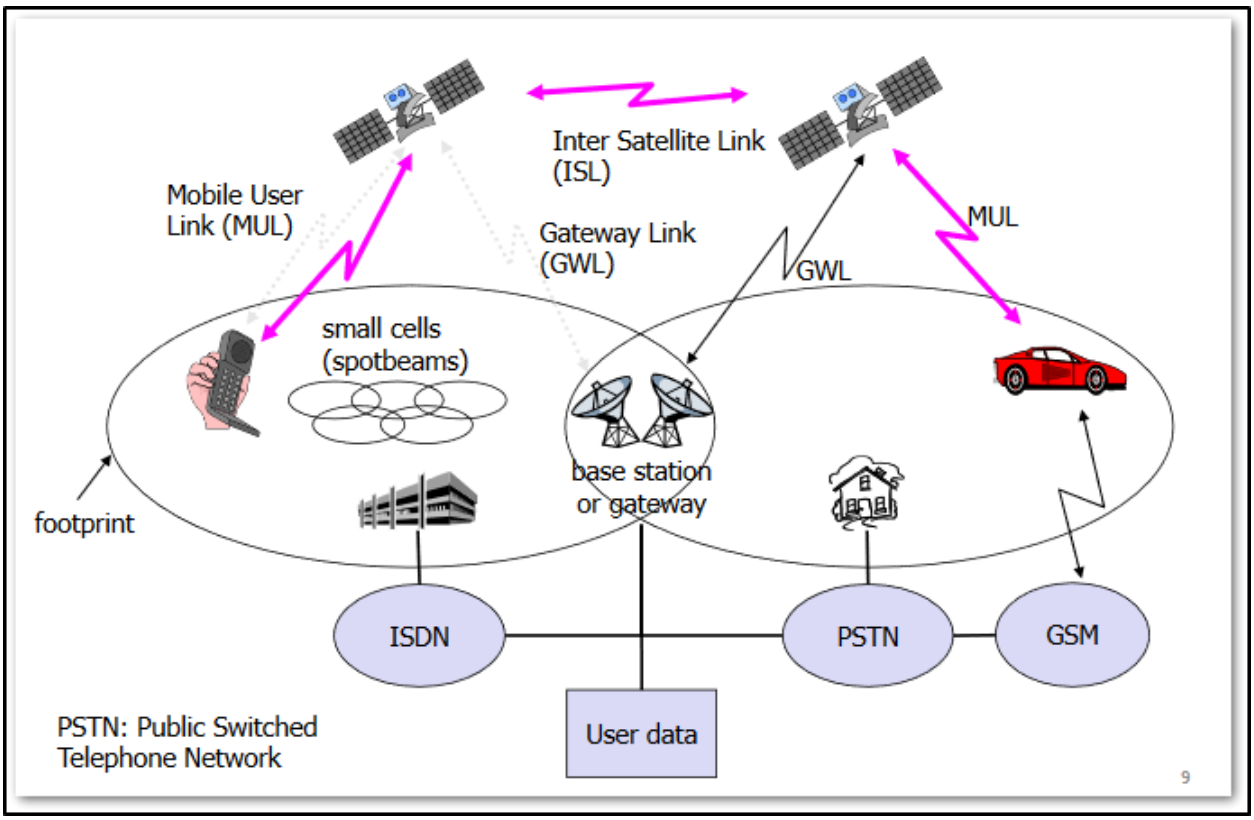
Uplink is the communication link from *transmitting earth station* to satellite.

Downlink is the communication link from satelliteto *receiving earth station*.

History of Satellite Communication

Year	Discription
1945	Arthur C. Clarke publishes an essay about "Extra Terrestrial Relays"
1957	First satellite SPUTNIK
1960	First reflecting communication satellite ECHO
1963	First geostationary satellite SYNCOM
1965	First commercial geostationary satellite "Early Bird" (INTELSAT I): 240 duplex telephone channels or 1 TV channel, 1.5 years lifetime
1976	Three MARISAT satellites for maritime communication
1982	First mobile satellite telephone system INMARSAT-A
1988	First satellite system for mobile phones and data communication INMARSAT-C
1993	First digital satellite telephone system
1998	Global satellite systems for small mobile phones

Classical Satellite Systems



- **Footprint** is overall coverage area of any satellite.
- **Base station or gateway** is central earth station that allows your networks or devices to connect to this and transmit/receive data via satellite network.
- **Gateway Link** is used to make communication between base station and satellite.
- **Mobile User Link:** The devices that are capable to directly talk to the satellite, use MUL built-in the device to communicate to the satellite.
- **Inter Satellite Link** is the media that satellites use to transmit data among themselves.

Altitudes of Orbits above the Earth

- There are 3 common types of satellite based on altitude, i.e. GEO, MEO & LEO

Orbit	Altitude	Missions possible
Low-Earth orbit LEO	250 to 1,500 km	Earth observation, meteorology, telecommunications (constellations)
Medium-Earth orbit MEO	10,000 to 30,000 km	Telecommunications (constellations), positioning, science
Geostationary Earth orbit GEO	35,786 km	Telecommunications, positioning, science
Elliptical orbit	Between 800 and 27,000 km	Telecommunications
Hyperbolic orbit	Up to several million km	Interplanetary missions

Satellite Orbits

Satellites		
GEO	*Altitude*	36,000 KM above earth
	Purpose	Commercial and military communication
	Orbital Period	23h 56m 4.091s
		3 Satellites can cover the earth
MEO	*Altitude*	10,255 KM
	Purpose	Telecommunication and navigation systems
	Orbital Period	5h 55m 48.4s
LEO	*Altitude*	1,469
	Purpose	Military intelligence and weather communications
	Orbital Period	1h 55m 17.8
		66 Satellites can cover the earth

Non Geostationary Orbits (NGSO) is the range orbital positions that satellite should maintain and should not make a stationary position to avoid *Van Allen radiation belts* that causes damage to satellite.

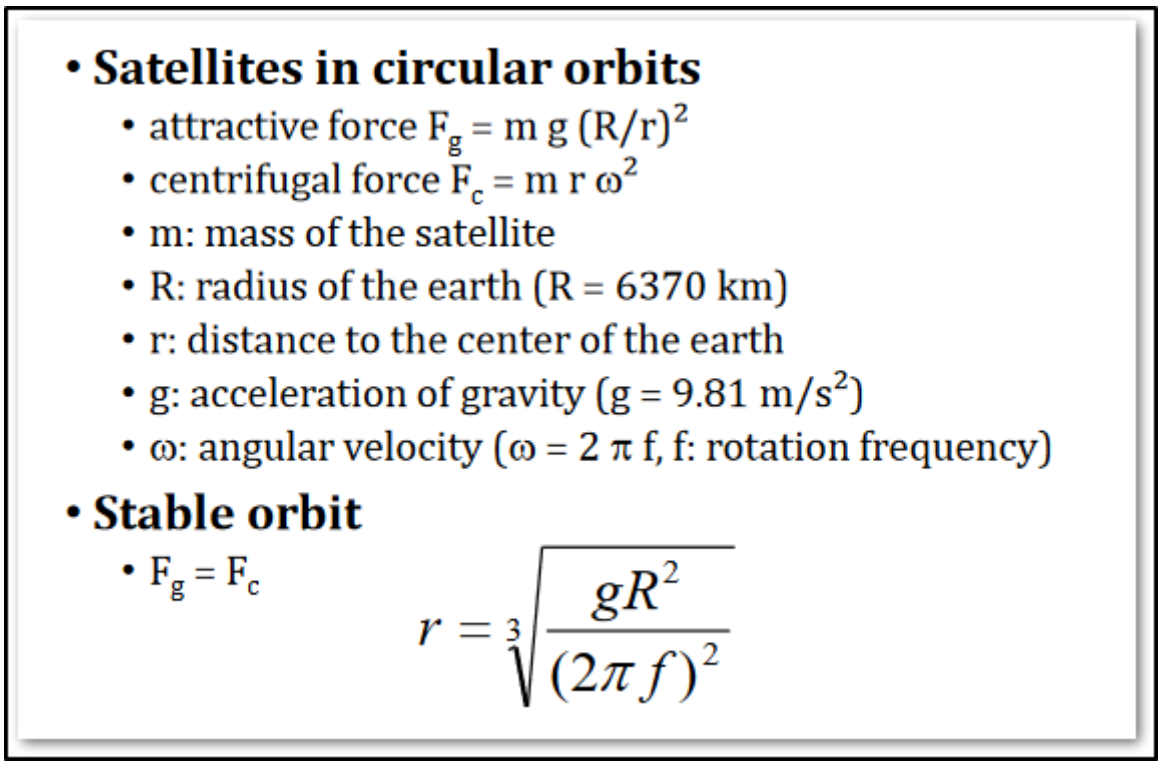
Orbital Period is thetime a satellite takes tocompleteone complete rotationinitsorbit.

Notice as altitude decreases, the velocity must be increased to minimize the gravitational effect.

Thecoveragearea (footprint) isinverselyproportionaltofrequency.Thefootprintwillbelargeifthefrequencyofdownlinkislow.

Why Satellites Remain in Orbits

Satellites are able to orbit around the planet because they are locked into speeds that are fast enough to defeat the downward pull of gravity.A satellite maintains its orbit by balancing two factors: its velocity (the speed it takes to travel in a straight line) and the gravitational pull that Earth has on it.



Effects of Rain on Signal

Rain heavily effects the wireless communication above 10GHz. In order to minimize this effect we maximize the power of uplink.

Why Uplink Frequency is always higher than Downlink Frequency?

Raineffectshigherfrequenciesmorethanloweronesotheyneedtobeboostedupmoretoovercomethepropagationlosses.TheEnergycanbegiventosignalmuchmoreeasilyonearththanonsatellite this is why uplink has more frequency.

Life of Satellite

A satellite has two life.

- **Design Life** is the predicted life of the electronic systems working in satellite.
- **Maneuver life** is the life during which full maneuver capabilities exist in satellite to change its position. It depends on fuel tank storage capacity & it is usually less than design life.

When the lifespan is over the satellite automatically move to the **graveyard orbit** where they revolve but do not perform any operations.

Why Do Microwaves are used for Satellite Communications?

- High frequency to carry data
- Long wavelength to penetrate atmosphere
- Require low power
- Resistant to interference
- Travel in straight line
- Easy production and detection

Why Two Frequencies for Uplink and Downlink in Satellite Communication?

It is to avoid interference between transmitter and receiver. Signals need to be operated on different frequencies.

Advantages and Disadvantages of Satellite Communication

Advantages	Disadvantages
Canreachoverlargegeographicalarea	Large upfront capital cost
Support mobile applications	Terrestrial break
Provision of services to remote and underdeveloped areas	Interference and propagation delay
Broadcast possibilities	Congestion of frequencies and orbits

Satellite Applications

- Military communication
- Telecommunication
- Satellite phone
- Cable TV
- GPS (Global Positioning System)
- Navigation
- Weather forecasting

Lecture – 04: Wireless LAN

Local Wireless Network Technology according to IEEE

The standard for Wireless LAN defined by IEEE is **802.11** and there are its sub-types. **802.11** was launched in 1997 having speed 1 to 2 Mbps with the frequency band 2.4 Ghz.

- 802.11a was launched in 1999 having speed 54Mbps with 5 GHz band. It used OFDM protocol.
- 802.11b frequency band was changed to 2.4 Ghz and the speed dropped to 11Mbps. It used DSSS protocol. The reach increased and speed dropped.
- 802.11g was launched in 2003 having speed 54Mbps with band 2.4 Ghz. It used OFDM protocol.
- 802.11n is latest, it has 2.4Ghz and 154Mbps speed. It used MiMo protocol.

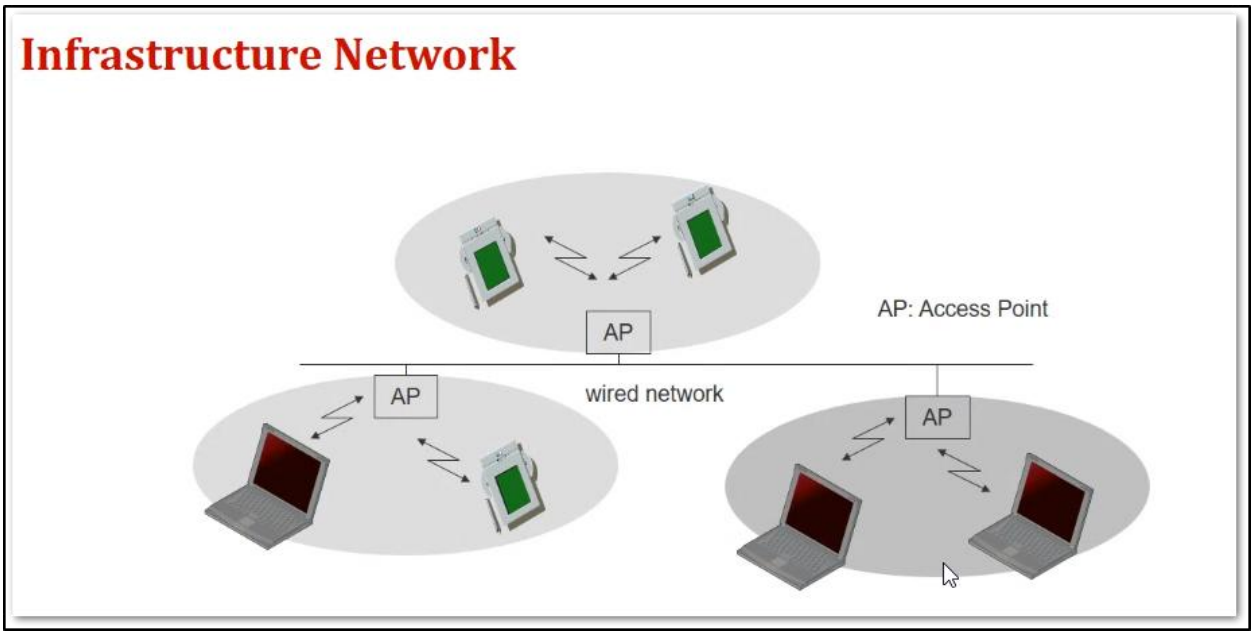
2/4 Ghz band frequency could be used all around the world. The 5 Ghz is controlled by countries and only could be used after purchasing license.

All the protocols are backward compatible.

WiFi stands for wireless fidelity. It is famous because it is compatible to almost every computing device.

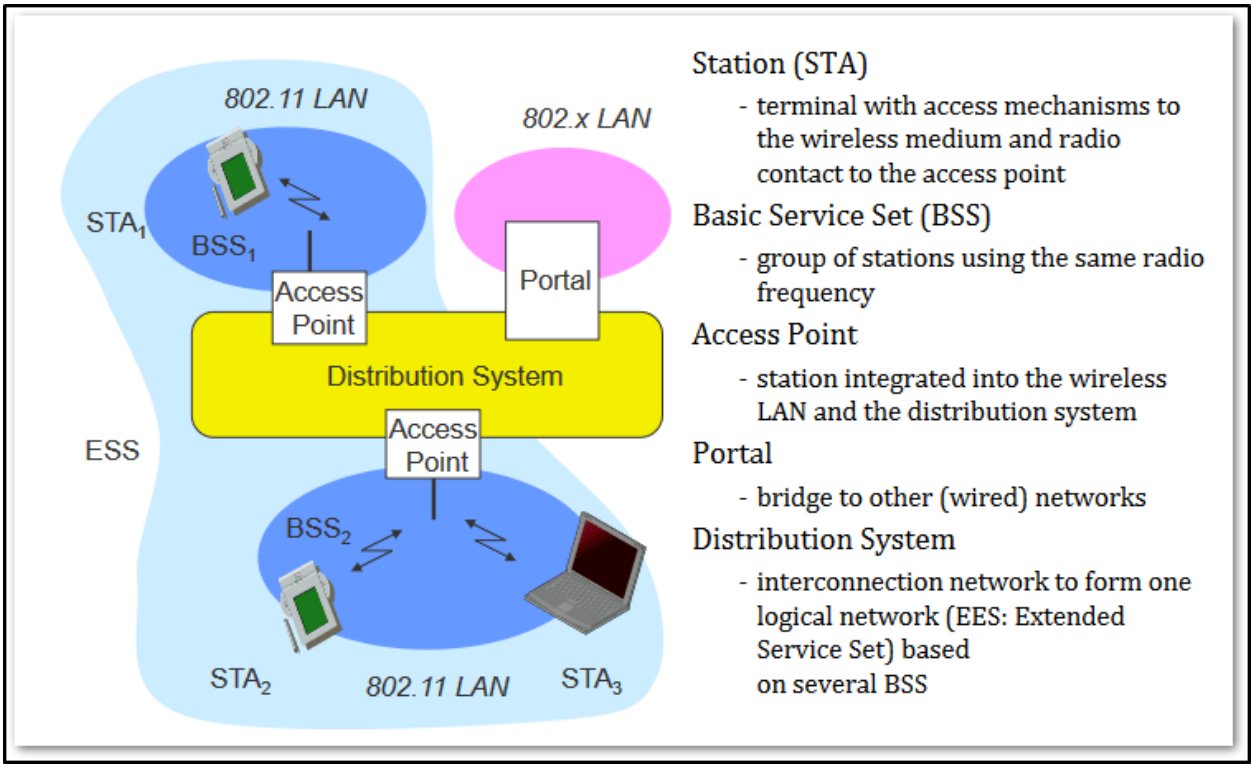
LiFi stands for light fidelity. Its speed is considered to be upto 10Ghz.

Infrastructure Network



The wireless network that has a backbone is called infrastructure WLAN. This backbone has multiple APs connected. This architecture uses both wireless technology and infrastructure technology.

802.11 -Architecture of an Infrastructure Network

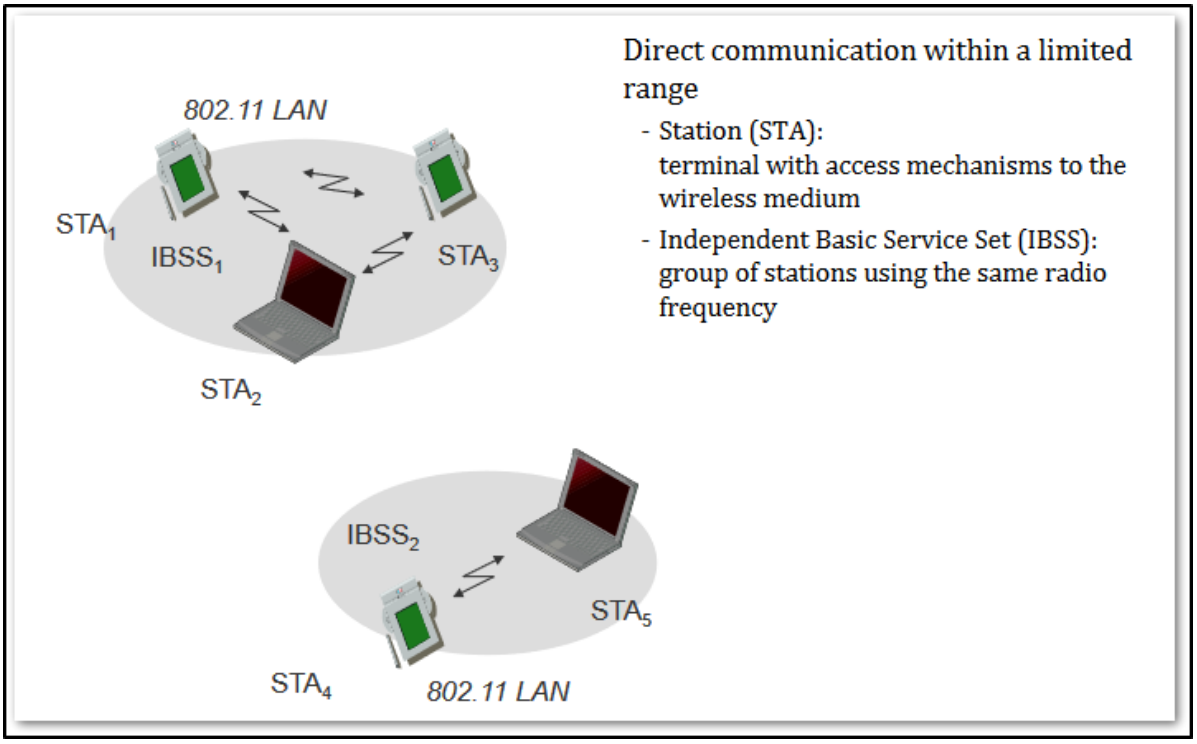


- **Distribution system** is the backbone of infrastructure.
- **Station** any device that has capability to connect to wireless network such as laptop, mobile, smart watch all are capable of wireless communication it is station.
- **Basic Service Set (BSS)** it is coverage area of one access point.
- **Extended Service Set (ESS)** the coverage are of more than one access point.
- **Access point** is the device that enable stations (devices) to connect to distribution system (backbone network).
- **Portal** a bridge between wireless and wired network.

Ad-Hoc Networks

It does not have any centralized controller. The devices are responsible for routing data and making communication.

802.11 – Architecture of an Ad-Hoc Network



Stations Transition

Transition types:

- **No transition:** Stationary or moves only within BSS
- **BSS transition:** Station (device) moves from one BSS to another BSS.
- **ESS transition:**A station moving from one ESS to another ESS still having access to the first ESS devices.

802.11 Services

802.11 services are divided into two types: distribution and integration.

Distribution Service

It is used to exchange MAC frames (Layer 2 data) from station in one BSS to station in another BSS.

Integration Service

It is used to integrate between 802.11 (Wireless) to 802.x (other) networks.

Other Services

Association Services

- **Association:** Establishes initial association between station and AP
- **Re-association:**Enables transfer of association from one AP to another, allowing station to move from one BSS to another / updates location en station and AP
- **Disassociation:** Association termination notice from station or AP

Access and Privacy Services

- **Authentication:** Establishes identity of stations to each other
- **De-authentication:** Invoked when existing authentication is terminated
- **Privacy:** Prevents message contents from being read by unintended recipient

MAC Service Data Unit Delivery (MSDU) Delivery

Responsible to ensure delivery of data to the STA

Lecture – 05: Mobile IP

Mobile IP

Basics

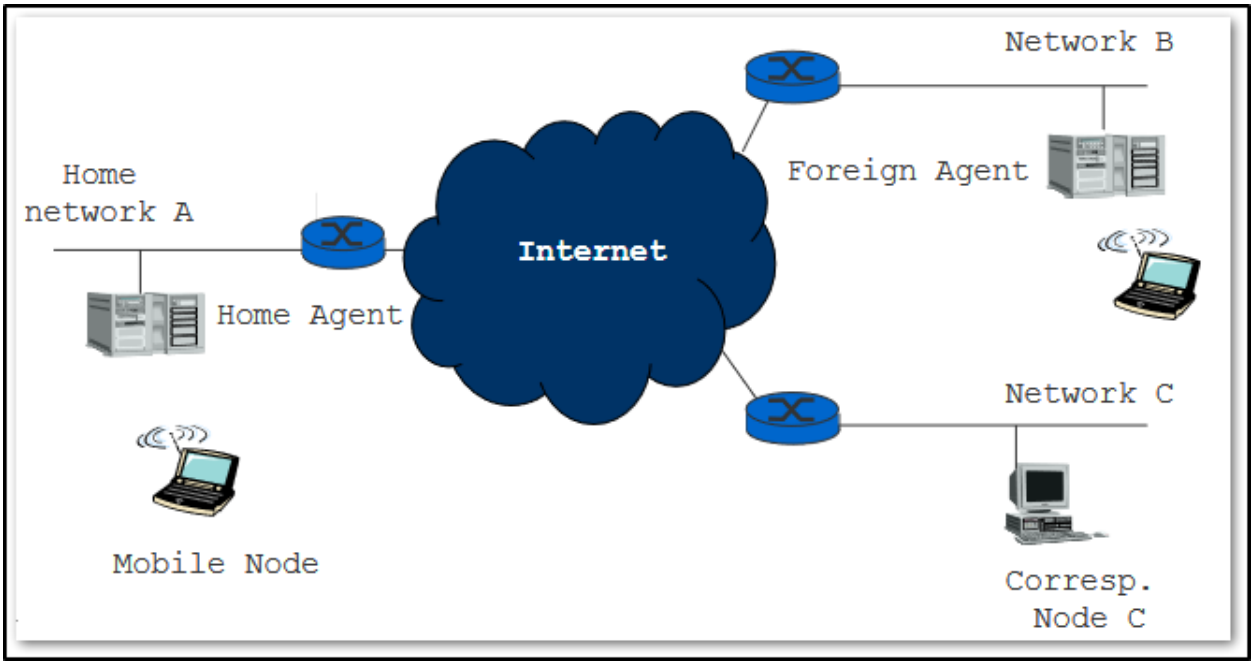
Using mobile IP any node can move from one network to another without affecting network architecture and communication with other nodes from the primary network.

Mobile IP allows a mobile host to move about without changing its **permanent**IP address. Each mobile host has a **homeagent**on its **home network** and Mobile host establishes a **care-of address** when it's away from home network.

Mobile IP Entities or Terminology

Mobile Node (MN): System(node)thatcanchangethepointofconnectiontothenetworkwithoutchangingitsIPaddress.

Home Agent (HA): SysteminthehomenetworkoftheMN,typicallyarouter. Tunnels IP datagrams to the CoA.



Foreign Agent (FA): SysteminttheforeignnetworkoftheMN,typicallyarouter. Forwards the tunneled datagrams to MN.

Care-of Address (CoA):IP address of the foreign agent that sends and receives mobile IP network traffic.

- When there is a packet from home network and it is sent to the device that has moved to foreign network, the packet is forward to the home agent (router) the home agent forwards this to foreign agent (router) and the address of this is **care-of address**.

- The other type of **care-of address** when the mobile node receives IP address (DHCP) and it sends this IP to the home agent (router) and this can also be the **care-of address**.

Care-of Address must be registered with home agent.

Correspondent Node(CN): Communication partner

Protocols

In order to support mobility, Mobile IP includes three capabilities:

1. Discovery
2. Registration
3. Tunneling

Discovery

Mobile / Foreign Agents send ICMP router advertisements periodically informing mobile nodes of its presence.

Registration

Mobile node recognizes that it is on a foreign network, acquires a Care-of-Address and requests its home agent to forward its data packets to the foreign agent.

Registration Process:

1. Mobile node request forwarding service by sending registration request to the foreign agent.
2. Foreign agent relays this request to the home agent.
3. Home agent accepts or denies the request and sends registration reply to the foreign agent.
4. Foreign agent relays this reply to Mobile node.

Tunneling

After registration, an IP tunnel is set up between the home agent and care-of-address of the mobile node.

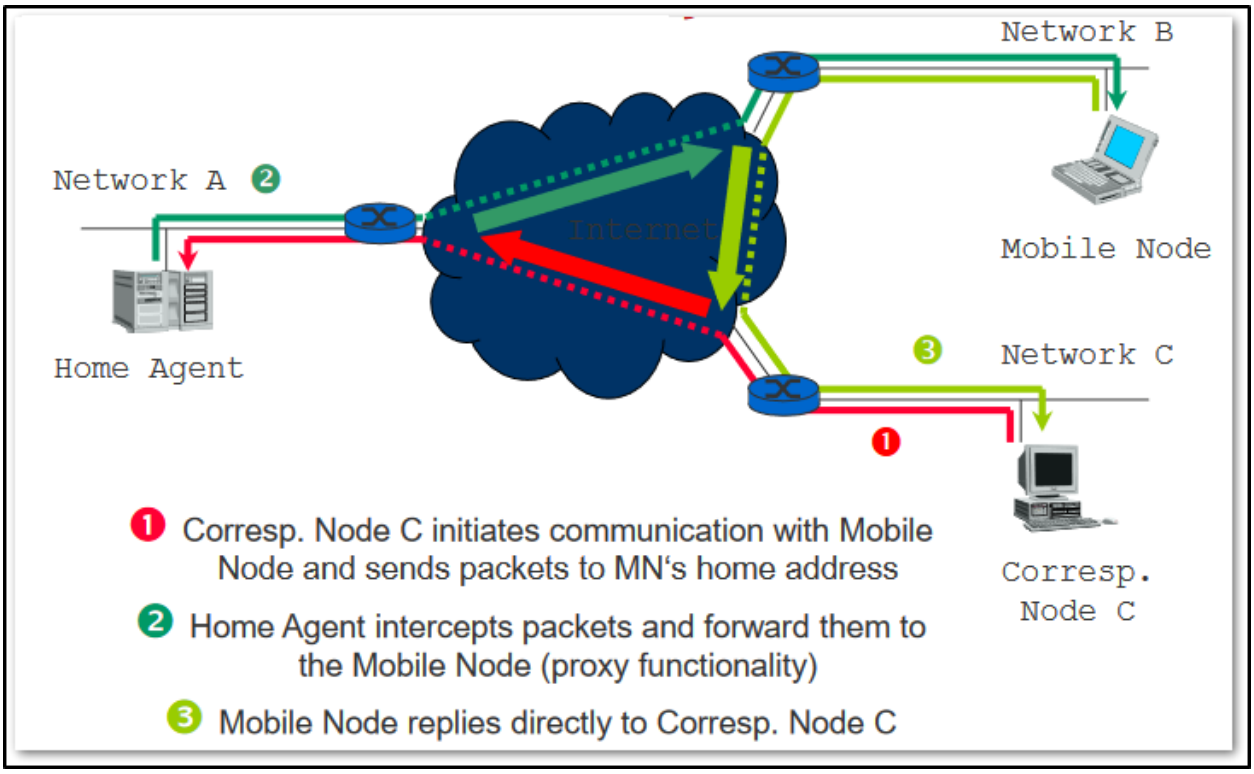
- Home agent receives packets destined to the mobile node, and forwards the packets to the foreign agent through the IP tunnel.
- Foreign agent or mobile node itself decapsulates the packet

IP-in-IP Tunneling

Packet to be forwarded is encapsulated in a new IP packet

In the new header:

- Destination = care-of-address
- Source = address of home agent


Network B
Network A
2
Internet
Mobile Node
Home Agent
3
Network C
1
Corresp.
Node C
1 Corresp. Node C initiates communication with Mobile Node and sends packets to MN's home address
2 Home Agent intercepts packets and forward them to the Mobile Node (proxy functionality)
3 Mobile Node replies directly to Corresp. Node C

Lecture – 06: MANET

Mobile Ad-Hoc Network (MANET)

MANET is collection of mobile nodes that are capable of changing their position on continuous basis. The nodes are self-forming, self-maintaining, and self-healing.

MANET is a network of mobile nodes that can change their location and configure themselves accordingly in order to maintain connectivity with all the previous and current sibling nodes.

Routing Protocols

Reactive Protocol

The routes are constructed on-demand of new route. The source nodes check the route in their routing table first (each node), if route is not available the route discovery process is initiated and if route is discovered the packet is sent if route is not discovered the packet is dropped.

In **dense** network the reactive routing protocol performs at its best.

Example: AODV (Ad hoc On-Demand Distance Vector)

Proactive Protocol

This protocol proactively reaches out to other nodes and gather their routing table and makes routing table for each node. The tables are actively maintained.
There is minimum traffic delay but overhead of network communication as after every 120 seconds routing tables are exchanged. The data packets movement gets highly effected.

Example: DSDV (destination sequenced distance vector)

Hybrid Protocol

It is combination of proactive and reactive. Reactive is used within one zone and proactive is used between zones.

Example : ZRP (zone routing protocol)

Distance Vector Routing Protocol

Distance-vector routing protocols measure the distance by the number of routers a packet has to pass, one router counts as one hop. The best path to all destinations are computed and updates are performed periodically.

It uses Bellman-Ford, Ford-Fulkerson, or DUAL FSM algorithms.

Ad-Hoc On-Demand Distance Vector (AODV) Protocol

It is dynamic, self-starting, multi-hop routing protocol for mobile nodes. It maintains only one route from source to destination and after a defined lifetime the route is expired if not used.

AODV defines 3 message types:

1. **Route Requests (RREQs)**: messages are used to initiate the route finding process. It also includes the last known sequence number for the destination.

2. **Route Replies (RREPs)**: messages are used to finalize the routes.
3. **Route Errors (RERRs):** messages are used to notify the network of a link breakage in an active route.

A routing table entry maintaining a *reverse path* is purged after a timeout interval A routing table entry maintaining a forward path is purged (if not used)for a active_route_timeout interval.

Maintaining Sequence Numbers

It is important to maintain sequence numbers in order to make this protocol loop-free. All nodes including destination must increment their sequence number.

Forwarding nodes update their stored sequence number when forwarding RREP when:

- The sequence number in the routing table is invalid
- The sequence number in the RREP message is greater than the stored number
- The sequence numbers are identical, but the route is marked as inactive
- The sequence numbers are the same, but the hop count is smaller for the RREP message.

AODV Operation

Route Requests (RREQ) are broadcasted it to its neighbors with initial TTL of 1. When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source.

When the intended destination receives a Route Request, it replies by sending a **Route Reply (RREP)** Route Reply travels along the reverse path set-up when Route Request is forwarded.

Link Failure & Route Error

Neighboring nodes periodically exchange hello message. When the next hop link in a routing table entry breaks, all active neighbors are informed. Link failures are propagated by means of **Route Error (RERR)** messages, which also update destination sequence numbers.

When source node receives the RERR, it initiates a new route discovery for destination using destination sequence number at least as large as sent with RERR message.

Performance of AODV

AODV does not retransmit data packets that are lost and hence does not guarantee packet delivery.

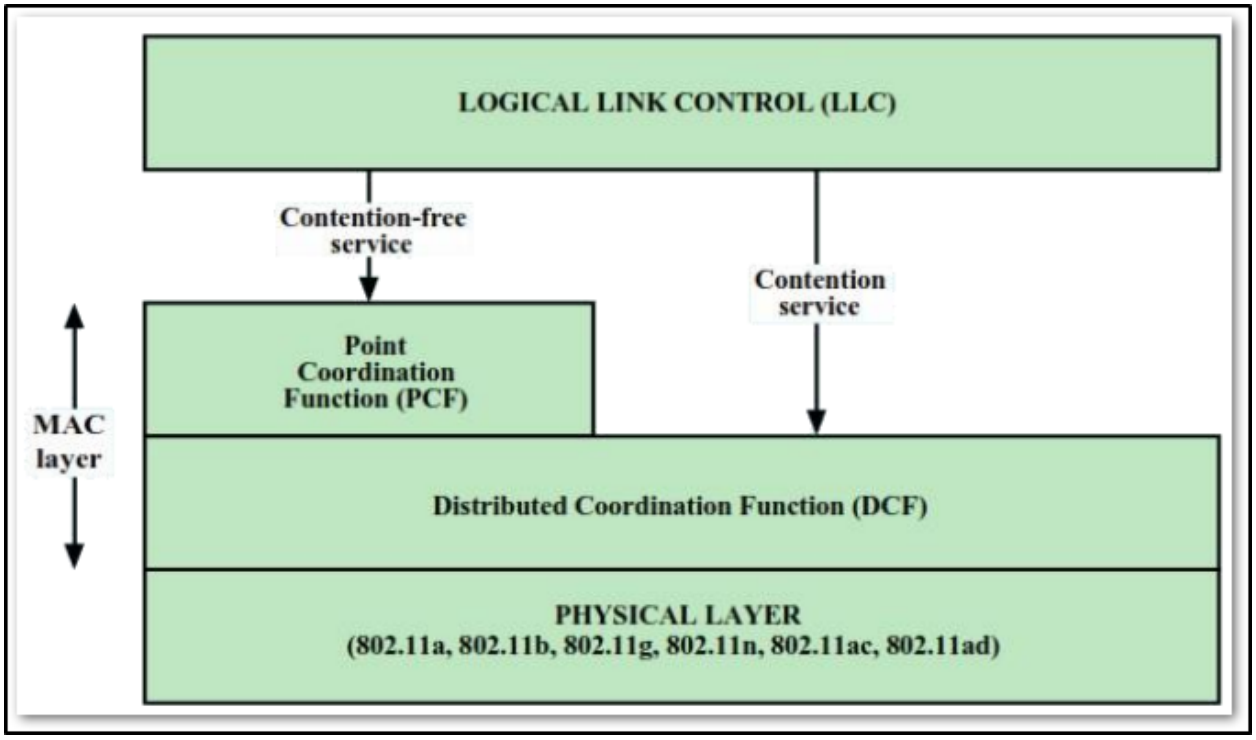
The overhead packets in AODV are due to RREQ, RREP and RERR messages. AODV needs much less number of overhead packets compared to DSDV. The number of overhead packets increases with increased mobility, since this gives rise to frequent link breaks and route discovery.

Destination Sequenced Distance Vector (DSDV) Protocol

- All nodes maintain a Route Table Entry for every other destination in the network
- Route Table Entry – contains next hop for a destination, number of hops to reach the destination, a sequence number
- Nodes broadcast routing updates
- Sequence Number – helps removing stale routes, and avoids loops

Lecture – 07: DCF & PCF

802.11 – MAC Layer



Distributed Coordination Function (DCF)

Distributed Coordination Function (DCF) is used for sharing access to the medium based on the CSMA/CA protocol for WLAN defined by IEEE 802.11 standard.

A node listens to the channel before transmission to determine whether someone else is transmitting. The receiving node sends an acknowledge packet (ACK) a short time interval after receiving the packet. If an ACK is not received, the packet is considered lost and a retransmission is arranged.

Priorities

- **SIFS (Short Inter Frame Spacing)** - highest priority, for ACK, CTS, polling response
- **PIFS (PCF IFS)** - medium priority, for time-bounded service using PCF
- **DIFS (DCF, Distributed Coordination Function IFS)** - lowest priority, for asynchronous data service

DCF Access Modes

DCF consists of a basic access mode as well as an optional RTS/CTS access mode.

DCF Basic Access

In basic access mode the node senses the channel to determine whether another node is transmitting before initiating a transmission If the medium is sensed to be free for a DCF inter-frame space (DIFS)

time interval the transmission will proceed If the medium is busy the node defers its transmission until the end of the current transmission.

The backoff timer is decreased as long as the medium is sensed to be idle for a DIFS, and frozen when a transmission is detected on the medium. When the backoff reaches 0, the station transmits it Packet.

A short inter-frame space (SIFS) is used to give priority access to ACK packets. When receiving a packet correctly an ACK packet is sent to the source node. If the source node does not receive an ACK it reactivates the backoff and retransmits the packet.

DCF RTS/CTS Access

The purpose of RTS/CTS exchange is to avoid long collisions since we don't have collision detection. The source node sends a request-to-send (RTS) packet to announce an incoming transmission. The destination node sends a clear-to-send (CTS) packet to source node for allowing transmission.

Point Coordination Function (PCF)

- AP polls stations on its list, and maintains control of the medium
    - Transmissions are separated by PIFS
    - Each CF-Poll is a license for one frame

Lecture – 08: Hidden Node and Exposed Node Problem

CSMA Problems in Wireless Medium

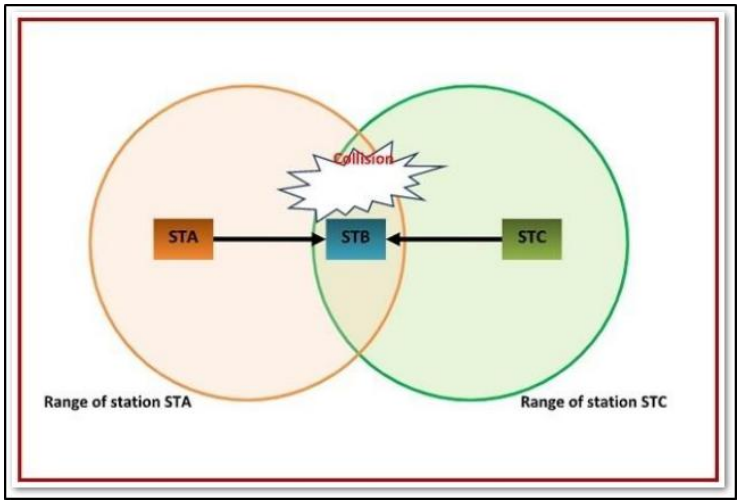
Collision detection is easy in wired networks but difficult in wireless medium.

With only one antenna/radio, nodes can only listen or send. Full duplex radios are extremely expensive. CSMA gives rise to hidden terminal and exposed terminal problems.

Hidden Node Problem

Other senders' information are hidden from the current sender, so that transmissions at the same receiver cause collisions.

The situation happens when two or more sending nodes outside the transmission range of each other transmit data to the same node in the next hop nearly at the same time, thus likely resulting in data collision at the receiving node. These sending nodes are hidden from each other because they are unable to detect the existence of one another.



Solution: Hidden Node Problem

RTS/CTS can help

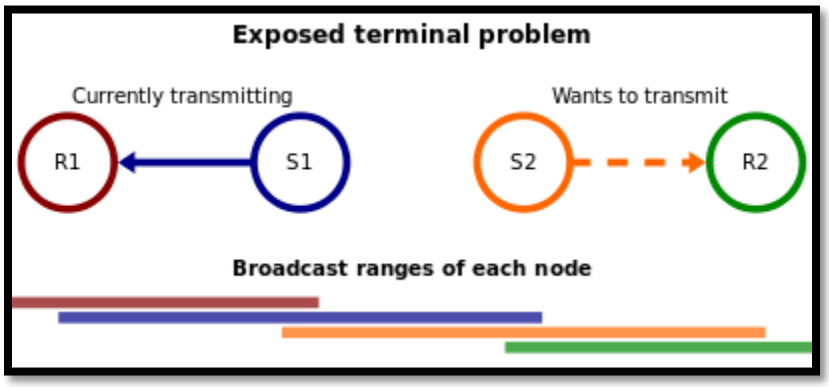
- Both A and C would send RTS that B would see first
- B only responds with one CTS (say, echoing A's RTS)
- C detects that CTS doesn't match and won't send

Exposed Node Problem

The sender mistakenly think the medium is in use, so that it unnecessarily defers the transmission.

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes because of co-channel interference with a neighboring transmitter. Consider an example

of four nodes labeled R1, S1, S2, and R2, where the two receivers (R1, R2) are out of range of each other, yet the two transmitters (S1, S2) in the middle are in range of each other. Here, if a transmission between S1 and R1 is taking place, node S2 is prevented from transmitting to R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor S1. However note that R2 could still receive the transmission of S2 without interference because it is out of range of S1.



Solution: Exposed Node Problem

The exposed terminal problem is solved by the MAC (medium access control) layer protocol IEEE 802.11 RTS/CTS.

Any station hearing the RTS is close to the transmitting station and remains silent long enough for the CTS. Any station hearing the CTS is close to the receiving station and remains silent during the data transmission.

Lecture – 09: DSSS & FHSS

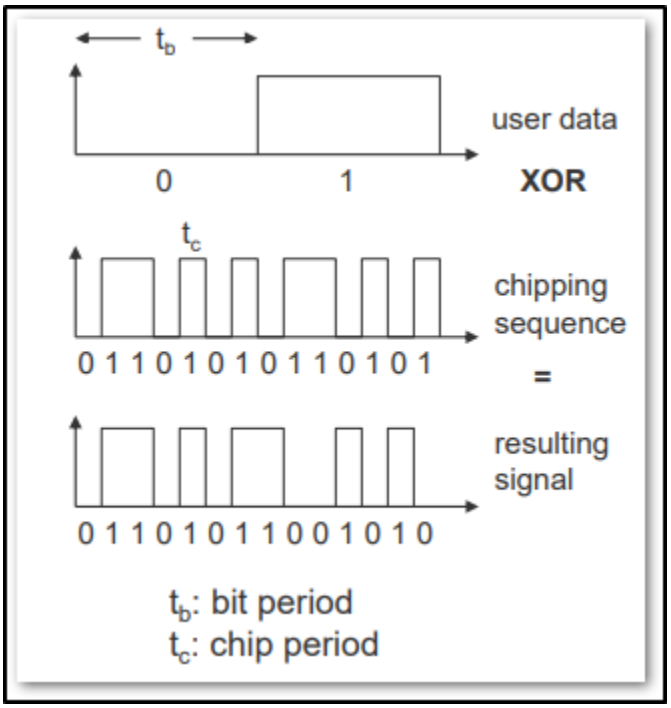
Spread Spectrum Technology

Spread spectrum uses wideband, noise-like signals that are hard to detect, intercept, or demodulate. Additionally, spread-spectrum signals are harder to jam (interfere with) than narrow band signals. This is the reason military has used it for so many years.

Direct sequence and frequency hopping are the most commonly used methods for the spread spectrum technology.

DSSS (Direct Sequence Spread Spectrum)

The carrier of the direct-sequence radio stays at a fixed frequency. Narrowband information is spread out into a much larger (at least 10 times) bandwidth by using a pseudo-random chip sequence. At the receiving end of a direct-sequence system, the spread spectrum signal is de-spread to generate the original narrowband signal.



Advantages

- Reduces frequency selective fading
- In cellular networks
    - Base stations can use the same frequency range
    - Several base stations can detect and recover the signal
    - Soft handover

Disadvantage

Precise power control necessary

FHSS (Frequency Hopping Spread Spectrum)

Frequency-hopping systems achieve the same results provided by direct-sequence systems by using different carrier frequency at different time. The frequency-hopping technique does not spread the signal, as a result, there is no processing gain.

The frequency hopper, however, is more difficult to synchronize. In these architectures, the receiver and the transmitter must be synchronized in time and frequency in order to ensure proper transmission and reception of signals.

The frequency hopper, however, is better than the direct-sequence radio when dealing with multipath.

It has two types:

- **Fast Hopping**: several frequencies per user bit
- **Slow Hopping**: several user bits per frequency

Advantages

- Simple implementation
- Uses only small portion of spectrum at any time

Disadvantages

- Not as robust as DSSS
- Simpler to detect

Lecture – 10: Packet Switching / Forwarding

Packet Switching

Packet switching is the transfer of small pieces of data across various networks. These data chunks or "packets" allow for faster, more efficient data transfer.

Packets arrive at one of the several inputs and have to be forwarded / switched to one of the available outputs.

Forwarding is the process of selecting an appropriate output port for a packet.

Challenges for Packet Switching

Efficient forwarding and routing in a dynamic network, and handling contention are three major challenges of packet switching.

Routing

Packet forwarding requires information this information is maintained via routing. Routing is the process of selecting a path for traffic in a network or between or across multiple networks.

Packet Switching / Forwarding Types

This could be performed by three approaches.

1. Datagram or connectionless
2. Virtual circuit or connection-oriented
3. Source routing

Datagram

Every packet contains all the information required to reach destination. Switches maintain forwarding table and translate global address to destination port. Each packet forwarded independently and this is connectionless approach.

If destination is not available the packet is discarded and sender is informed.

Virtual Circuit

In this approach a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit.

In this connection-oriented model packets are delivered in order and each packet does not have to contain all the information rather packet only contain a small identifier making overhead small.

Signaling

Signaling is the process of creating virtual circuit tables using setup message.

1. The setup message is forwarded from host A to host B.
2. Each switch creates an entry in VC table with VCI.
3. Host B accepts connection and sends back an ACK.

    - In ACK, everyone communicates its choice of VCI to its upstream neighbor.
4. Host A acknowledges ACK.
5. Data transmission begins and data packets, each node then puts the VCI of its downstream neighbor.

Virtual circuit tables are maintained for each connection including source / destination port and incoming / outgoing virtual circuit identifier.

Source Routing

Packet header contains sequenceof address/ports on path from source to destination. Switches read, use, and then discard directions. This model is used in some system area networks (SANs).

- If arrival rate for a certain output is greater than the output capacity, then contention occurs
- If arrival rate of packets is too high to cause buffer overflow, then congestion occurs

Lecture – 11: Global Positioning System (GPS)

GPS

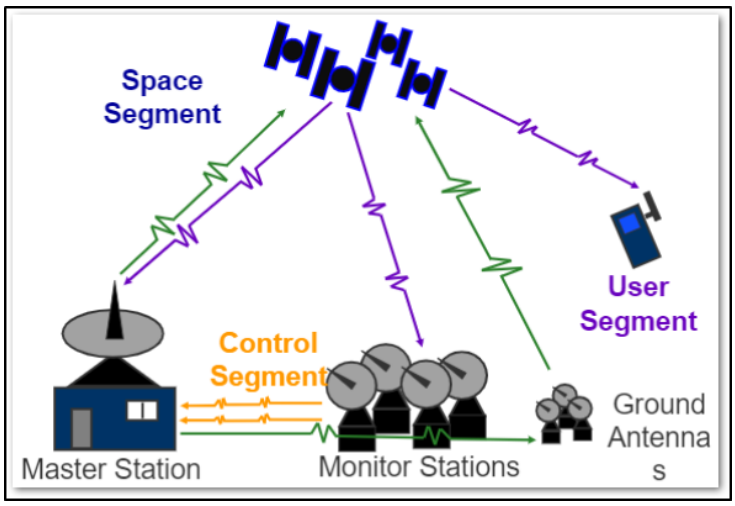
GPA is a Constellation of Earth-Orbiting Satellites Maintained by the United States Government for the Purpose of Defining Geographic Positions On and Above the Surface of the Earth. It consists of Three Segments:

1. User segment
2. Control segment
3. Space segment

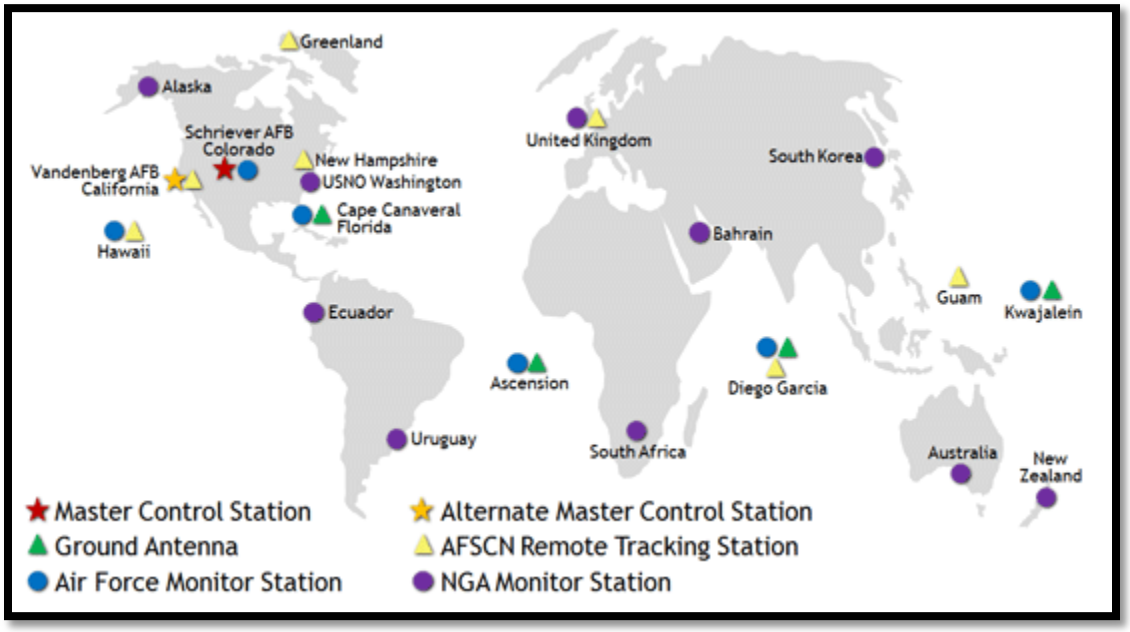
Four Primary Functions of GPS

1. Position and coordinates.
2. The distance and direction between any two waypoints.
3. Travel progress reports.
4. Accurate time measurement.

Segments of the GPS



Control Segment



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. The locations of these facilities are shown in the map above.

Space Segment

The GPS space segment consists of a constellation of satellites transmitting radio signals to users. The United States is committed to maintaining the availability of at least 24 operational GPS satellites, 95% of the time

User Segment

The user segment consists of the GPS receiver equipment, which receives the signals from the GPS satellites and uses the transmitted information to calculate the user's three-dimensional position and time.

Trilateration

Trilateration is the process of determining your position based on the intersection of spheres. When a receiver receives a signal from one of the satellite, it calculates its distance from the satellite considering a 3-D sphere with the satellite located at the center of the sphere. Once the receiver does the same with 3 other GPS satellites, the receiver then proceeds to the intersection point of the 3 spheres to calculate its location.

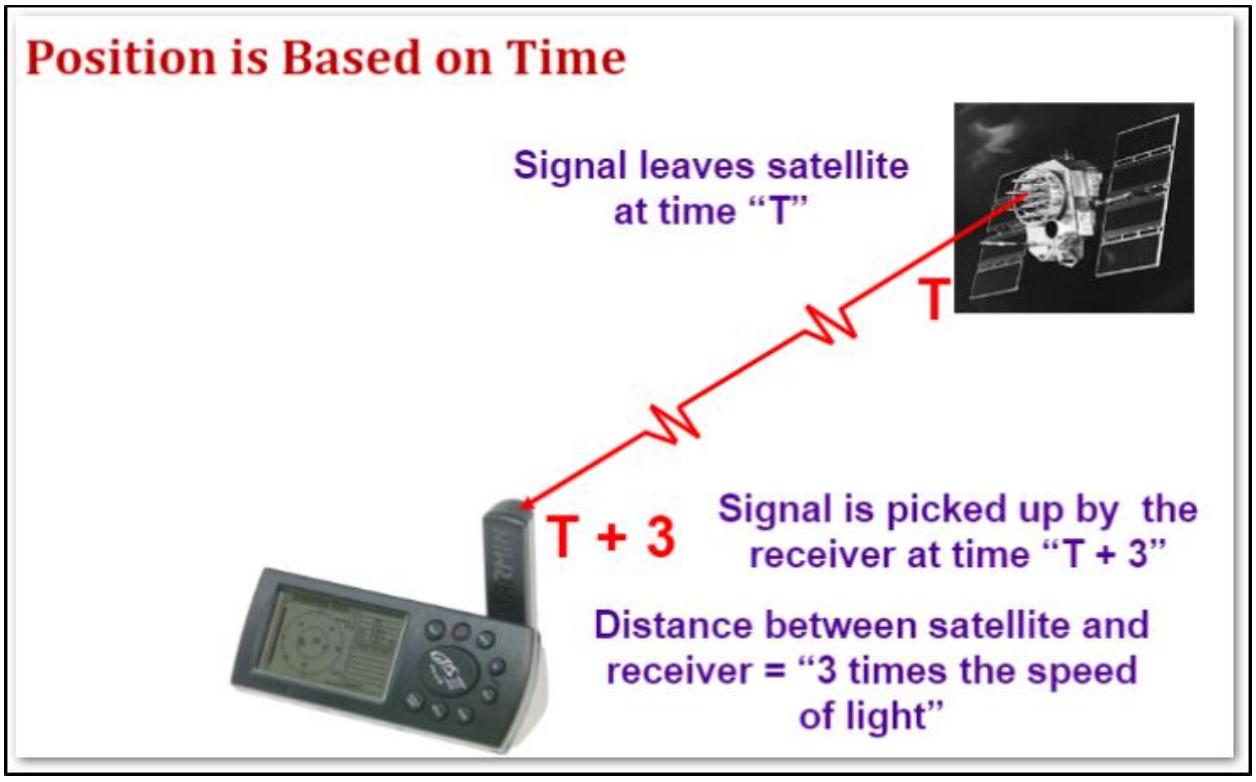
GPS Working

GPS utilizes atomic clock and revolves 11,000 miles above earth.

Satellites send data to earth which are picked up by a receiver Signals arrive at different times based on the distance from the satellite. Receiver needs to determine distance to 3 satellites.

Distance is calculated using Distance = Speed (of light) * Time.

Time is determined using pseudo random codes of 3 satellites. Each satellite transmits a unique “pseudo random” code at extremely precise time intervals. Receiver knows each satellite’s pseudo random code and when they are sent receiver determines the time delay it takes to match the expected satellite pseudo random code with the received pseudo random code.



Lecture – 12: Fifth Generation (5G)

5G

5G is the latest generation of cellular mobile communications. It targets; high data rate, reduced latency, energy saving, higher system capacity, and massive device connectivity.

5G networks achieved 10Gb which is faster than current cable network.

Generations Comparison

Features	1G	2G	3G	4G	5G
Start / Development	1980s	1991	1998	2009	2015
Technology	Analog transmission	Digital transmission	WCDMA	LTE, WiMax	MIMO
Use	Make phone calls	Send text messages	Internet access on mobile devices	Video conferencing, HD TV, Gaming, IP telephony	-

5G Technologies

Technologies used ins 5G are:

1. Millimeter waves
2. Small cells
3. Massive MIMO
4. Beamforming

Millimeter waves

5G enable higher speed is by using unused bands at the top of the radio spectrum. These high bands are known as Millimeter waves. Its frequency range is from 30GHz to 300GHz. These waves are susceptible to interference and can be absorbed by plants and rain. It also cannot penetrate walls.

Small cells

Millimeter waves have shorter range, therefore the cells are limited to smaller size.

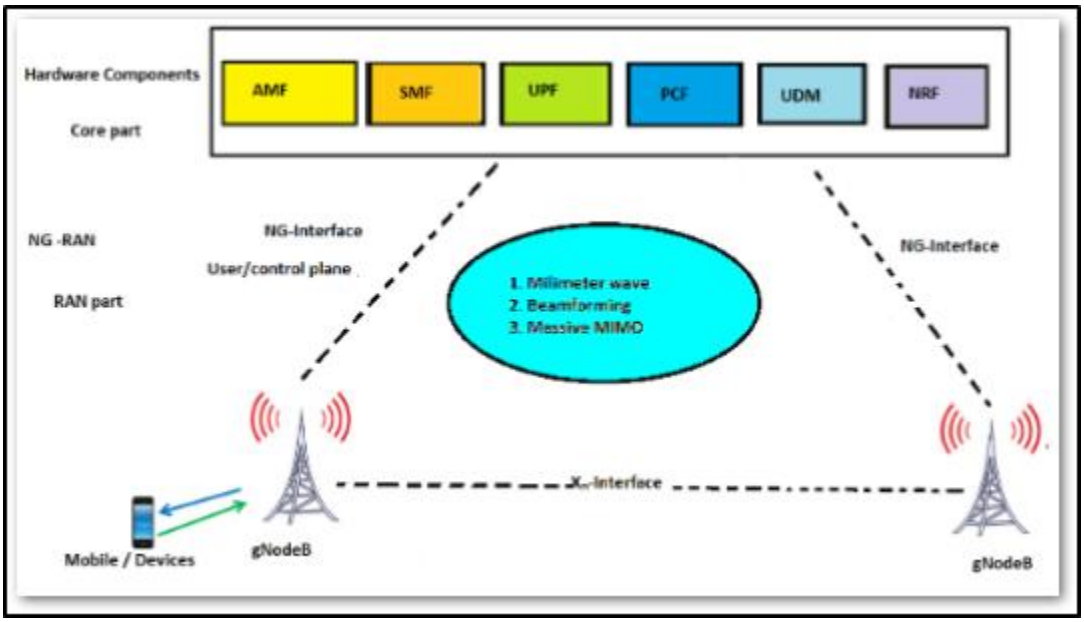
Massive MIMO

MIMO stands for “Multiple Input, Multiple Output”. It is antenna technology for wireless communication in which multiple antennas are used at both the transmitter and receiver.

Beamforming

Beamforming is used to prevent interference. Instead of broadcasting signals in all directions, beamforming allows a base station to send a focus stream of data to a specific user.

5G Architecture



- The lower gNodeBpart in the figure is called as Next Generation Network or NR-RAN (Next Generation Radio Access Network).
- gNodeBis also called as RAN part because it is directly connected to the hardware components.
- The hardware components or the upper layer is also core part.

gNodeB

It is like an antenna or towers where devices will connect.

Xn-Interface

Interface between two gNodeB.

NG-Interface

NG-Interface is user/control plane which is going to get connected to gNodeBand hardware components.

- User plane is used in terms of calling or usage of internet.
- Control plane is used for controlling, billing authentication or providing channel.

Hardware Components

The hardware is completely packet switching that means it is working on IPs. It is directly connected to gNodeB.

There are 6 hardware components used in 5G.

- **AMF (Access and Mobility Function):** Provide Authentication.
- **SMF (Session Management Function):** Manages sessions, QoS, and allocates IPs.
- **UPF (User Plane Function):** Manages call connectivity functions.
- **PCF (Policy and Control Function):** Keep record of bandwidth usage, sites visited and day-to-day activity of user the user.

- **UDM (Unified Data Management):** It looks after networks.
- **NRF (Network Repository Function):** Provides registration and discovery function.

Advantages of 5G

- Increased bandwidth (high data rate)
- Increased speed
- Reduced latency
- Massive device capacity

Disadvantages of 5g

- Technology issue
- Costly
- Security issues
- Competency

5G Applications

- IoT
- Virtual Reality
- SMART CARS
- Medicine
- Smart Cities
- Drones

Top Countries with 5G

China, South Korea, UK, Germany, US, Switzerland, Denmark, Finland, Iceland, Norway, Sweden.