Syllabus: Wireless LAN: Transmission Medium for WLANs, MAC Problems, Hidden and Exposed Terminals, Near and Far Terminals, Infrastructure and Ad-hoc Networks, IEEE 802.11- System Architecture, Protocol Architecture, Physical Layer, Concept of Spread Spectrum, MAC and its Management, Power Management, Security. Mobile IP: Unsuitability of Traditional IP; Goals, Terminology, Agent Advertisement and Discovery, Registration, Tunneling Techniques. Ad-hoc Network Routing: Ad-hoc Network Routing v/s Traditional IP Routing, Types of Routing Protocols, Examples: AODV, DSDV, DSR, ZRP.

WIRELESS LAN:

WANs are Wide Area Networks which cover a wider area such a city, or a limited area greater than LAN. Wireless WLANs use radio, infrared and microwave transmission to transmit data from one point to another without cables. Therefore WLAN offers way to build a Local Area Network without cables. This WLAN can then be attached to an already existing larger network

Fundamentals of WLANs: The technical issues in WLANs must be understood in order to appreciate the difference between wired networks and wireless networks. The use of WLANs and their design goals are then studied. The types of WLANS, their components and their basic functionalities are also detailed.

IEEE 802.11 Standards: IEEE 802.11 standard is a prominent standard of WLANs, the. The medium access control (MAC) layer and the physical layer mechanisms are explained.

HIPERLAN Standard: It is also a WLAN standard, HIPERLAN standard, which is a European standard based on radio access.

Bluetooth: Bluetooth enables personal devices to communicate with each other in the absence of infrastructure.

WLAN Fundamentals: While both portable terminals and mobile terminals can move from one place to another, portable terminals are accessed only when they are stationary.

Mobile Terminals (MTs), on the other hand, are more powerful, and can be accessed when they are in motion. WLANs aim to support truly mobile work stations.

WLAN USES

Wireless computer networks are capable of offering versatile functionalities. WLANs are very flexible and can be configured in a variety of topologies based on the application. Some possible uses of WLANs are described below.

- Users would be able to surf the Internet, check e-mail, and receive Instant Messages on the move.
- In areas affected by earthquakes or other disasters, no suitable infrastructure may be available on the site. WLANs are handy in such locations to set up networks on the fly.
- There are many historic buildings where there has been a need to set up computer networks. In such places, wiring may not be permitted or the building design may not be conductive to efficient wiring. WLANs are very good solutions in such places.

DESIGN GOALS

The following are some of the goals which have to be achieved while designing WLANs –

- **Operational simplicity** – Design of wireless LANS must incorporate features to enable a mobile user to quickly set up and access network services in a simple and efficient manner.

- **Power efficient operation** – The power-constrained nature of mobile computing devices such as laptops and PDAs necessitates the important requirement of WLANs operating with minimal power consumption. Therefore, the design of WLAN must incorporate power-saving features and use appropriate technologies and protocols to achieve this.

- **License-free operation** – One of the major factors that affects the cost of wireless access is the license fee for the spectrum in which a particular wireless access technology operates. Low cost of access is an important aspect for popularizing a WLAN technology.

- **Tolerance to interference** – The proliferation of different wireless networking technologies both for civilian and military applications have led to a significant **increase in the interference level** across the radio spectrum.

The WLAN design should account for this and take appropriate measures by way of selecting technologies and protocols to operate in the presence of interference.

- **Global Usability** – The design of the WLAN, the choice of technology, and the selection of the operating frequency spectrum should take into account the prevailing **spectrum restriction** in countries across the world. This ensures the acceptability of the technology across the world.

- **Security** – The inherent broadcast nature of wireless medium adds to the requirement of security features to be included in the design of WLAN technology.

- **Safety requirements** – The design of WLAN technology should follow the safety requirements that can be classified into the following.

    - Interference to medical and other instrumentation devices.
    - Increased power level of transmitters that can lead to health hazards.

A well-designed WLAN should follow the power emission restrictions that are applicable in the given frequency spectrum.

- **Quality of service requirements** – Quality of Service (**QoS**) refers to the provisioning of designated levels of performance for multimedia traffic. The design of WLAN should take into consideration the possibility of **supporting a wide variety** of traffic, including multimedia traffic.

- **Compatibility with other technologies and applications** – The interoperability among different LANS is important for efficient communication between hosts operating with different LAN technologies. Incorporate

ADVANTAGES OF WIRELESS LOCAL AREA NETWORK (WLAN)

- It is a reliable type of communication. As WLAN reduces physical wires so it is a flexible way of communication.
- WLAN also reduces the cost of ownership. It is easier to add or remove workstation.
- It provides high data rate due to small area coverage. You can also move workstation while maintaining the connectivity. For propagation, the light of sight is not required.

- The direction of connectivity can be anywhere i.e. user can connect devices in any direction unless it is in the range of access point.
- Easy installation and user need don't need extra cables for installation. WLAN can be useful in disasters situation e.g. earthquake and fire. People can still communicate through the wireless network during a disaster.
- It is economical because of the small area access. If there are any building or trees then still wireless connection works.

DISADVANTAGES OF WIRELESS LOCAL AREA NETWORK (WLAN)

- WLAN requires license. It has a limited area to cover.
- Government agencies can limit the signals of WLAN if required. This can affect data transfer from connected devices to the internet.
- If the number of connected devices increases then data transfer rate decreases. WLAN uses radio frequency which can interfere with other devices which use radio frequency. If there is rain or thunder then communication may interfere.
- Attackers can get access to the transmitted data because wireless LAN has low data security. Signals may be affected by the environment as compared to using fiber optics.
- The radiation of WLAN can be harmful to the environment.
- As WLAN uses access points and access points are expensive than wires and hubs. Access points can get signals of nearest access points.
- It is required to change the network card and access point when standard changes.
- LAN cable is still required which acts as the backbone of the WLAN. Low data transfer rate than wired connection because WLAN uses radio frequency.
- Chances of errors are high. Communication is not secure and can be accessed by unauthorized users.

TRANSMISSION MEDIUM FOR WLANS

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.

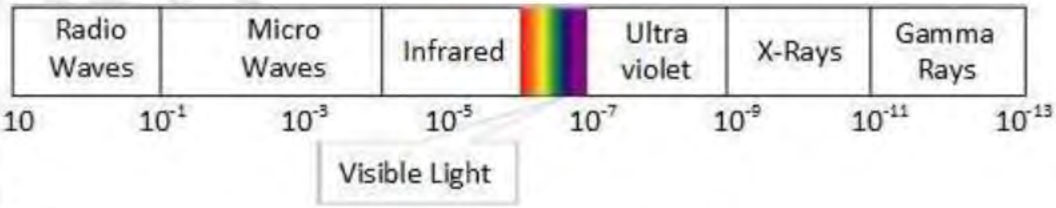


Figure 3.1: Electromagnetic Spectrum

RADIO TRANSMISSION

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1 mm to 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back. The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.

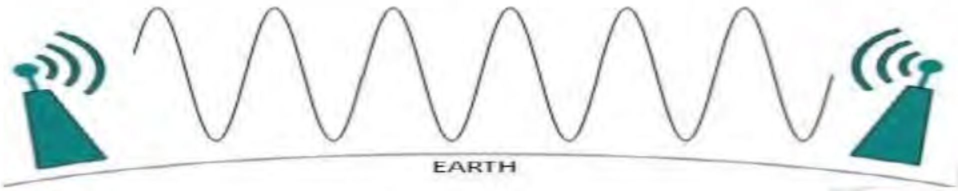


Figure 3.2: Radio Transmission

Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.

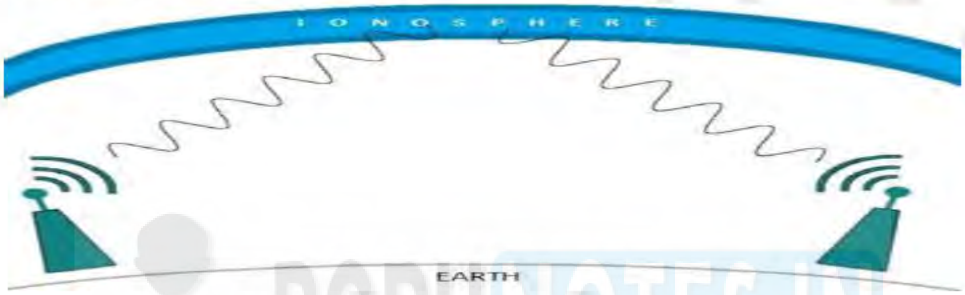


Figure 3.3: Radio Transmission

MICROWAVE TRANSMISSION

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.

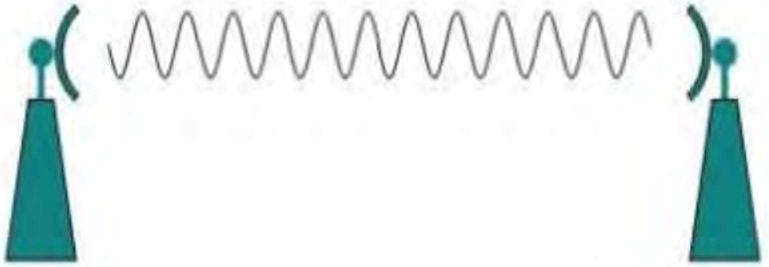


Figure 3.4: Microwave Transmission

Microwave antennas concentrate the waves making a beam of it. As shown in figure 3.4, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

INFRARED TRANSMISSION

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

LIGHT TRANSMISSION

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line. Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector need to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.

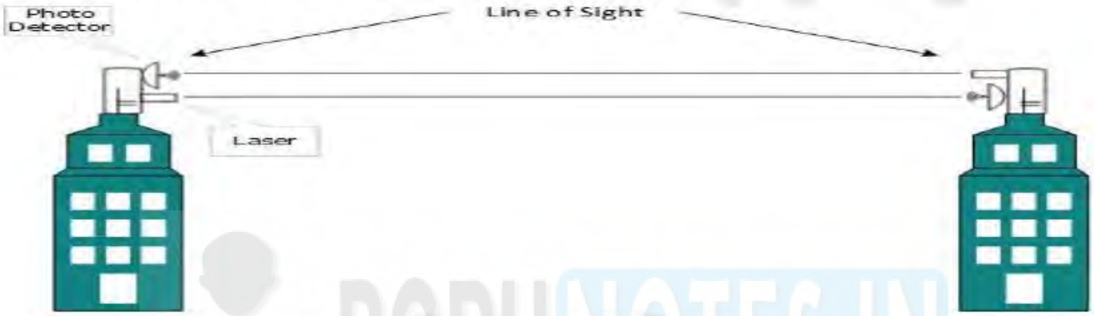


Figure 3.5: Light Transmission

Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver). Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path. Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

MAC PROBLEMS

The Media Access Control (MAC) data communication protocol sub-layer, also known as the Medium Access Control, is a sub layer of the Data Link Layer specified in the seven-layer OSI model (layer 2). The hardware that implements the MAC is referred to as a Medium Access Controller. The MAC sub-layer acts as an interface between the Logical Link Control (LLC) sub layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

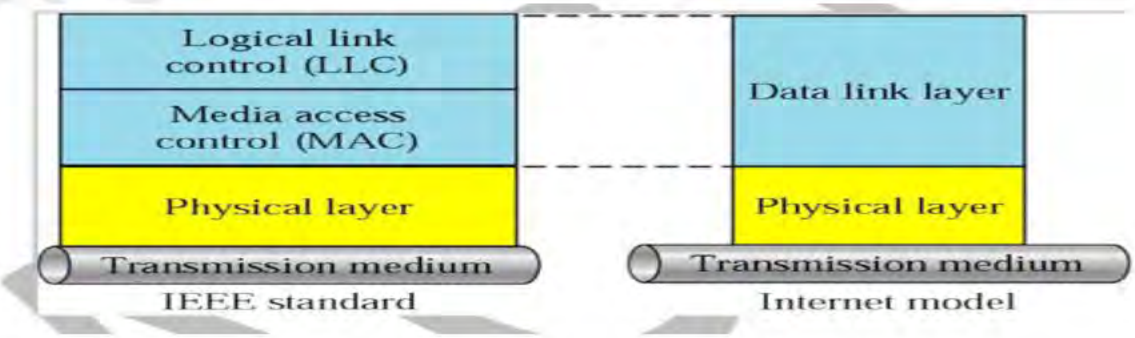


Figure 3.6: Media Access Control (MAC)

MOTIVATION FOR A SPECIALIZED MAC

One of the most commonly used MAC schemes for wired networks is carrier sense multiple access with collision detection (CSMA/CD). In this scheme, a sender senses the medium (a wire or coaxial cable) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal. But this scheme doest work well with wireless networks. The problems are:

- Signal strength decreases proportional to the square of the distance
- The sender would apply CS and CD, but the collisions happen at the receiver

It might be a case that a sender cannot "hear" the collision, i.e., CD does not work Furthermore, it might not work, if a terminal is "hidden

HIDDEN TERMINAL PROBLEM

A wireless network with lack of centralized control entity, sharing of wireless bandwidth among network access nodes i.e. medium access control (MAC) nodes must be organized in decentralized manner. The hidden terminal problem occurs when a terminal is visible from a wireless access point (APs), but not from other nodes communicating with that AP. This situation leads the difficulties in medium access control sub layer over wireless networking.

Consider a wireless networking, each node at the far edge of the access point's range, which is known as A, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, C. These nodes are known as hidden. The problem is when nodes A and C start to send packets simultaneously to the access point B. Because the nodes A and C are out of range of each other and so cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point. To overcome the hidden node problem, RTS/CTS handshaking (IEEE 802.11 RTS/CTS) is implemented in conjunction with the Carrier sense multiple accesses with collision avoidance (CSMA/CA) scheme. The same problem exists in a MANET.

Consider the scenario of wireless networking with three wireless devices (e.g. mobile phones) as shown below.

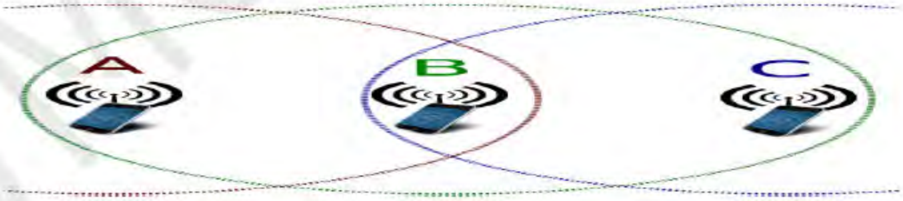


Figure 3.7: Hidden Terminal Problem

The transmission range of access point A reaches at B, but not at access point C, similarly transmission range of access point C reaches B, but not at A. These nodes are known as hidden terminals. The problem occurs when nodes A and C start to send data packets simultaneously to the access point B. Because the access points A and C are out of range of each other and resultant they cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point B due to the hidden terminal problem.

The hidden terminal analogy is described as follows:

- Terminal A sends data to B, terminal C cannot hear A.

- Terminal C wants to send data to B, terminal C senses a "free" medium (CS fails) and starts transmitting.
- Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission to B.
- Terminal A is "hidden" from C and vice versa.

Exposed Terminal Problem: In wireless networks, when a node is prevented from sending packets to other nodes because of a neighboring transmitter is known as the exposed node problem.

Consider the below wireless network having four nodes labeled A, B, C, and D, where the two receivers are out of range of each other, yet the two transmitters (B, C) in the middle are in range of each other. Here, if a transmission between A and B is taking place, node C is prevented from transmitting to D as it concludes after carrier sense that it will interfere with the transmission by its neighbor node B. However note that node D could still receive the transmission of C without interference because it is out of range from B. Therefore, implementing directional antenna at a physical layer in each node could reduce the probability of signal interference, because the signal is propagated in a narrow band.

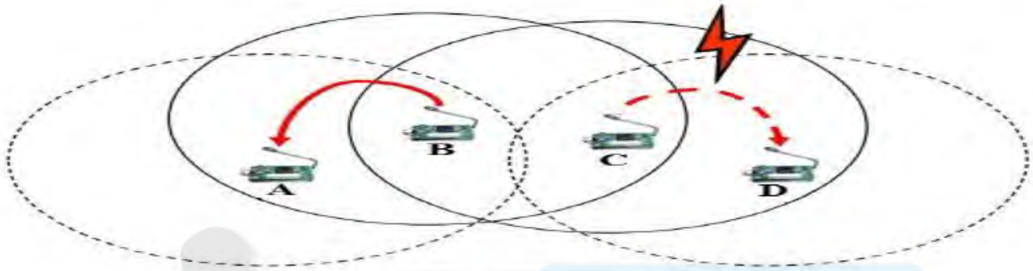


Figure 3.8: Exposed Terminal Problem

The exposed terminal analogy is described as follows:

- B sends to A, C wants to send to another terminal D not A or B
- C senses the carrier and detects that the carrier is busy.
- C postpones its transmission until it detects the medium as being idle again
- But A is outside radio range of C, waiting is not necessary
- C is "exposed" to B

Hidden terminals cause collisions, where as Exposed terminals causes' unnecessary delay.

HIDDEN V/S EXPOSED TERMINAL PROBLEM

Let us consider the following arguments:

- In the case of hidden terminal problem, unsuccessful transmissions result from collisions between transmissions originated by a node such as node A which cannot hear the ongoing transmissions to its corresponding node B. The probability of such a collision is proportional to the total number of terminals hidden from node A.

- In the case of exposed terminal, unsuccessful transmissions result from nodes such as node A being prevented from transmitting, because their corresponding node is unable to send a CTS. Again such unsuccessful transmissions are proportional to the number of exposed terminals. Both these events lead to degradation of a node's throughput.

NEAR AND FAR TERMINALS

Consider the situation where, A and B are both sending with the same transmission power.

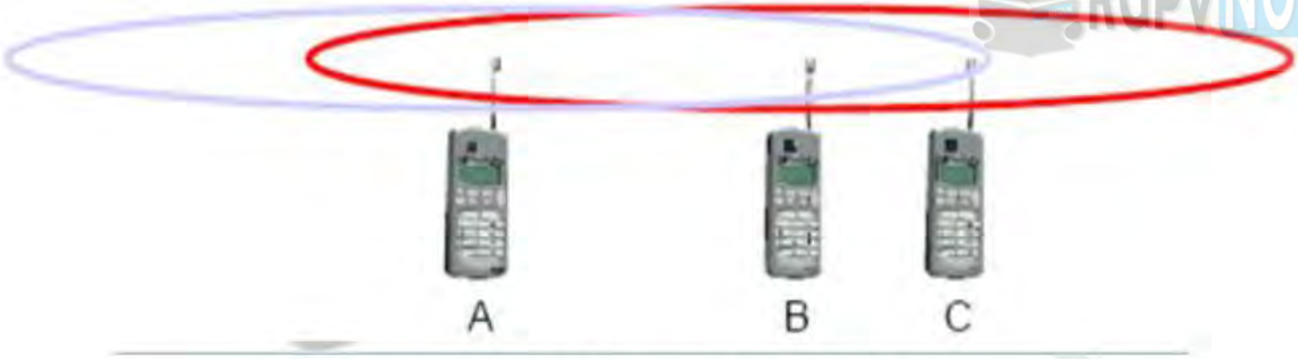
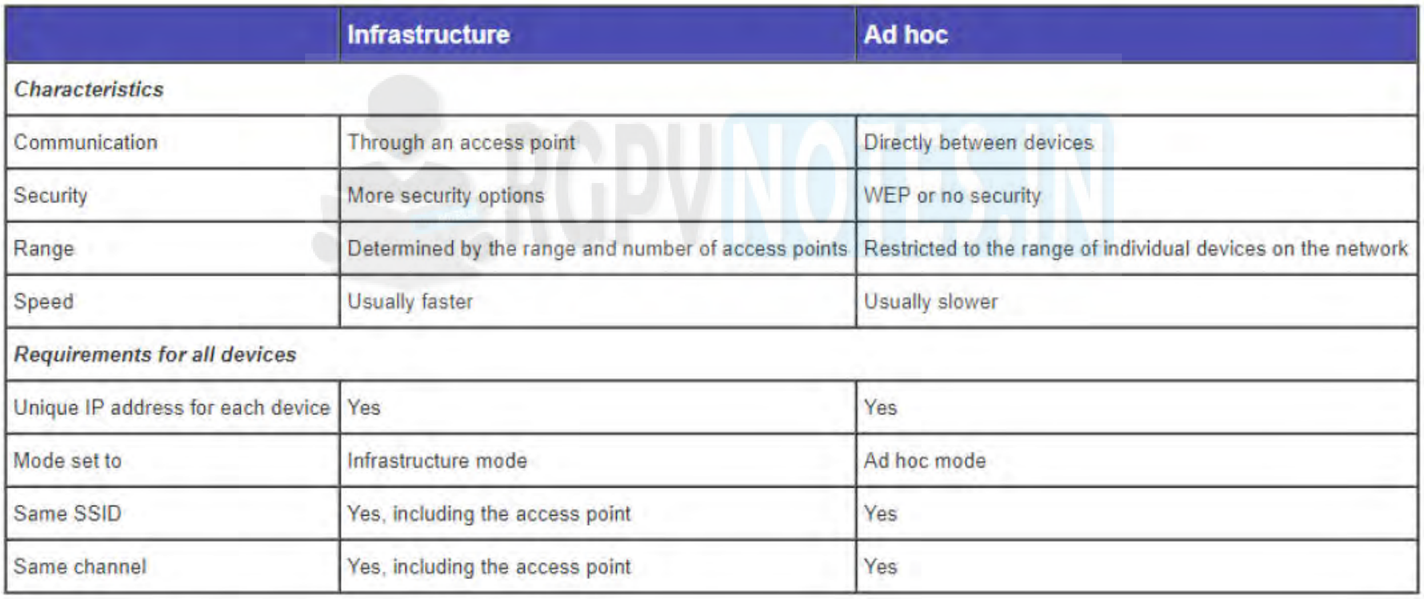


Figure 3.9: Near and Far Terminals

- Signal strength decreases proportional to the square of the distance
- B's signal drowns out A's signal making C unable to receive A's transmission
- If C is an arbiter for sending rights, B drown out A's signal on the physical layer making C unable to hear out A.

The near/far effect is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength for which Precise power control is to be implemented

Table 3.1: Comparison between Infrastructure and Ad hoc Networks



	Infrastructure	Ad hoc
Characteristics		
Communication	Through an access point	Directly between devices
Security	More security options	WEP or no security
Range	Determined by the range and number of access points	Restricted to the range of individual devices on the network
Speed	Usually faster	Usually slower
Requirements for all devices		
Unique IP address for each device	Yes	Yes
Mode set to	Infrastructure mode	Ad hoc mode
Same SSID	Yes, including the access point	Yes
Same channel	Yes, including the access point	Yes

IEEE 802.11

The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available. As the standard's number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. This means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to higher layers to maintain interoperability.

The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic. Candidates for physical layers were infra red and spread spectrum radio transmission techniques.

SYSTEM ARCHITECTURE

Wireless networks can exhibit two different basic system architectures as shown in infrastructure-based or ad-hoc. Figure 3.10 shows the components of an infrastructure and a wireless part as specified for IEEE 802.11. Several nodes, called stations (STAi), are connected to access points (AP). Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a basic service set (BSSi). The example shows two BSSs – BSS_1 and BSS_2 which are connected via a distribution system.

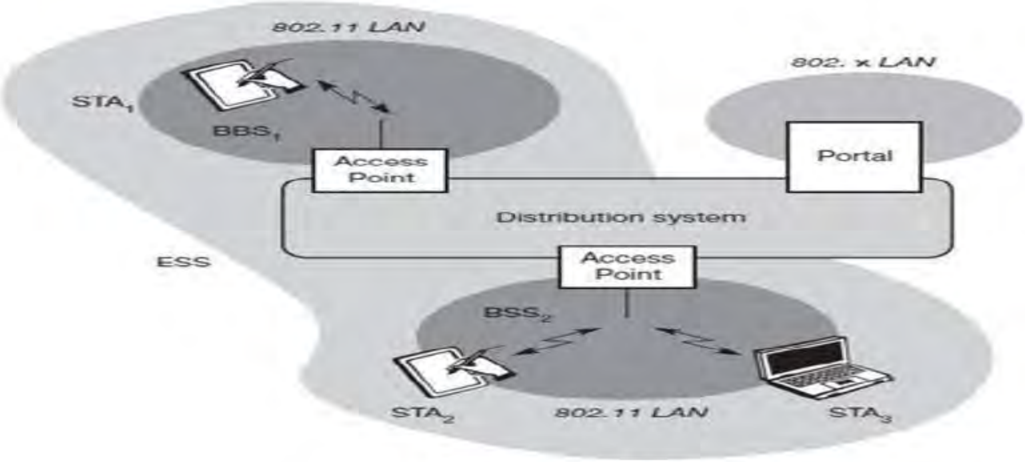


Figure 3.10: System Architecture

A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS) and has its own identifier, the ESSID. The ESSID is the 'name' of a network and is used to separate different networks. Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.

The architecture of the distribution system is not specified further in IEEE 802.11. It could consist of bridged IEEE LANs, wireless links, or any other networks. However, distribution system services are defined in the standard (although, many products today cannot interoperate and needs the additional standard IEEE 802.11f to specify an inter access point protocol. Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs.

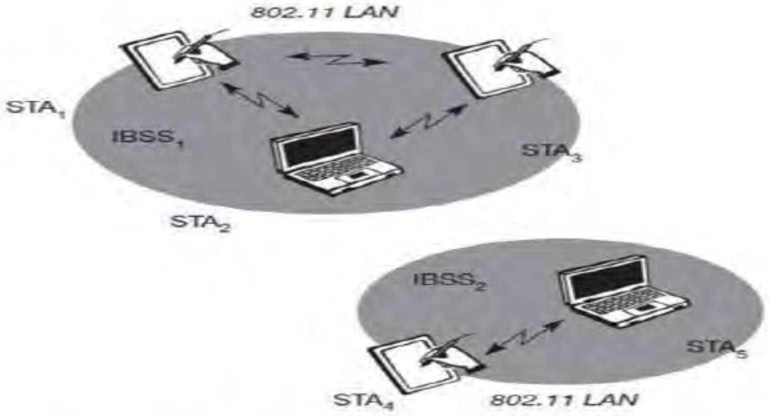


Figure 3.11: Wireless System Architecture

APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service. In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2. This means that STA3 can communicate directly with STA2 but not with STA5. Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies (then the IBSSs could overlap physically). IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN 1 or Bluetooth.

PROTOCOL ARCHITECTURE

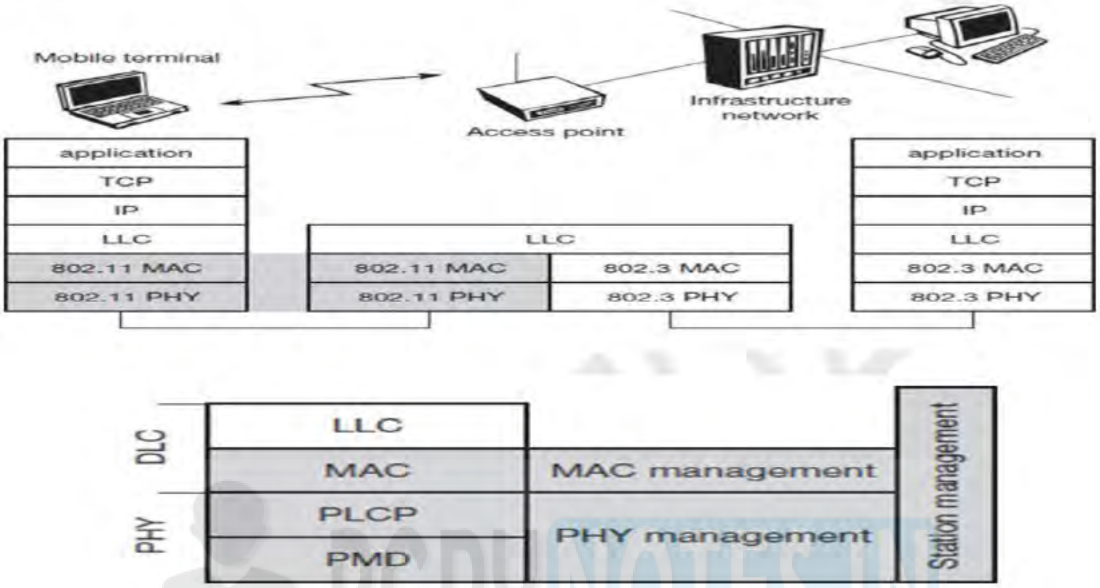


Figure 3.12: Protocol Architecture

As indicated by the standard number, IEEE 802.11 fits seamlessly into the other 802.x standards for wired LANs Figure shows the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge. Applications should not notice any difference apart from the lower bandwidth and perhaps higher access time from the wireless LAN. The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes. The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media. In many of today's networks, no explicit LLC layer is visible. Further details like Ether type or sub-network access protocol (SNAP) and bridging technology are explained.

The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do. The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sublayer PMD. The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption. The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sublayer handles modulation and encoding/decoding of signals.

Apart from the protocol sublayers, the standard specifies management layers and the station management. The MAC management supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power. MAC management also maintains the MAC management information base (MIB).

The main tasks of the PHY management include channel tuning and PHY MIB maintenance. Finally, station management interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

TERMINOLOGIES

- **Mobile Node (MN):** It is the hand-held communication device that the user caries e.g. Cell phone.
- **Home Network:** It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
- **Home Agent (HA):** It is a router in home network to which the mobile node was originally connected
- **Home Address:** It is the permanent IP address assigned to the mobile node (within its home network).
- **Foreign Network:** It is the current network to which the mobile node is visiting (away from its home network).
- **Foreign Agent (FA):** It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent who delivers it to the mobile node.
- **Correspondent Node (CN):** It is a device on the internet communicating to the mobile node.
- **Care of Address (COA):** It is the temporary address used by a mobile node while it is moving away from its home network.

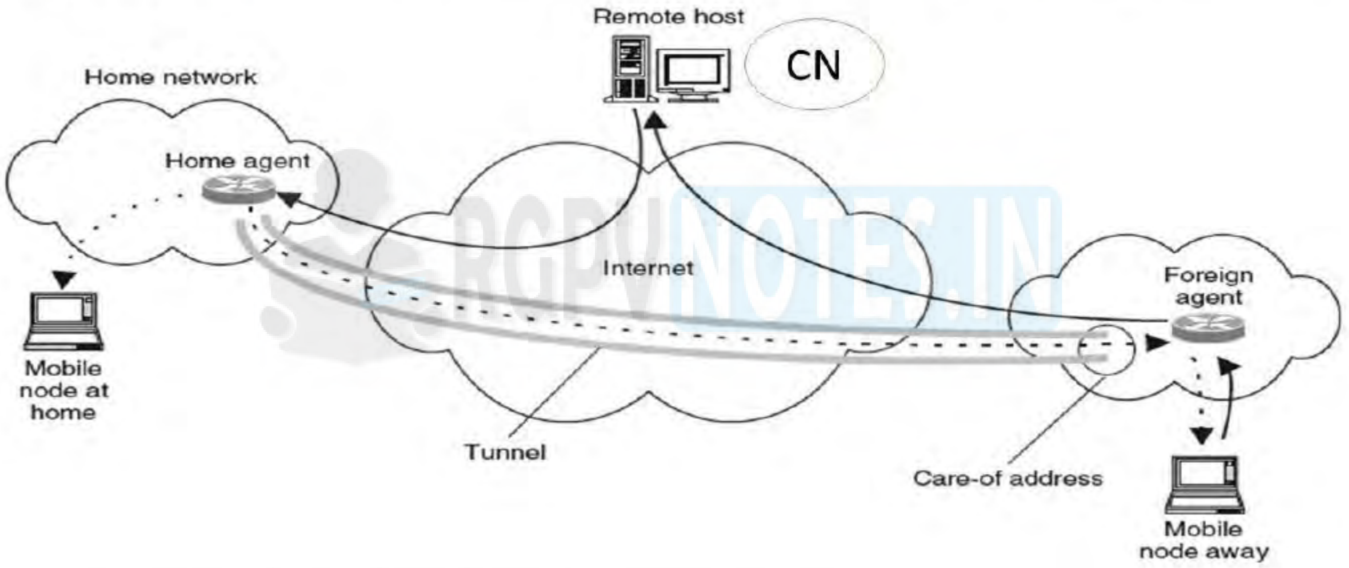


Figure 3.13: Mobile IP

WORKING

Correspondent node sends the data to the mobile node. Data packets contain correspondent node's address (Source) and home address (Destination). Packets reach to the home agent. But now mobile node is not in the home network, it has moved into the foreign network. Foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling. Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

ADHOC NETWORK

An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer coordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

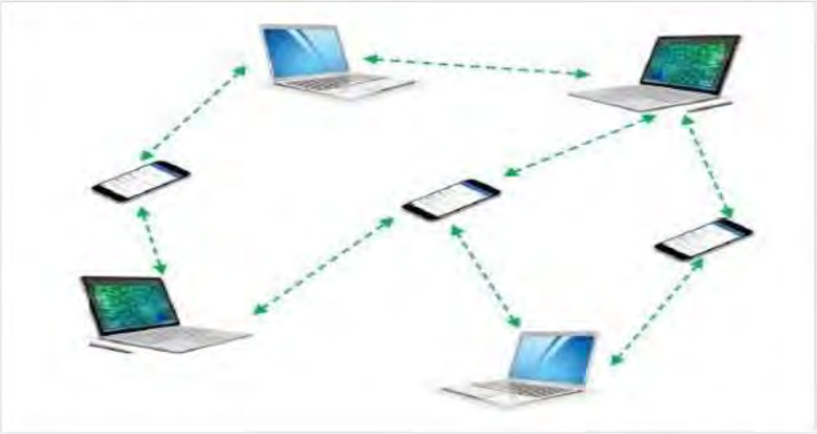
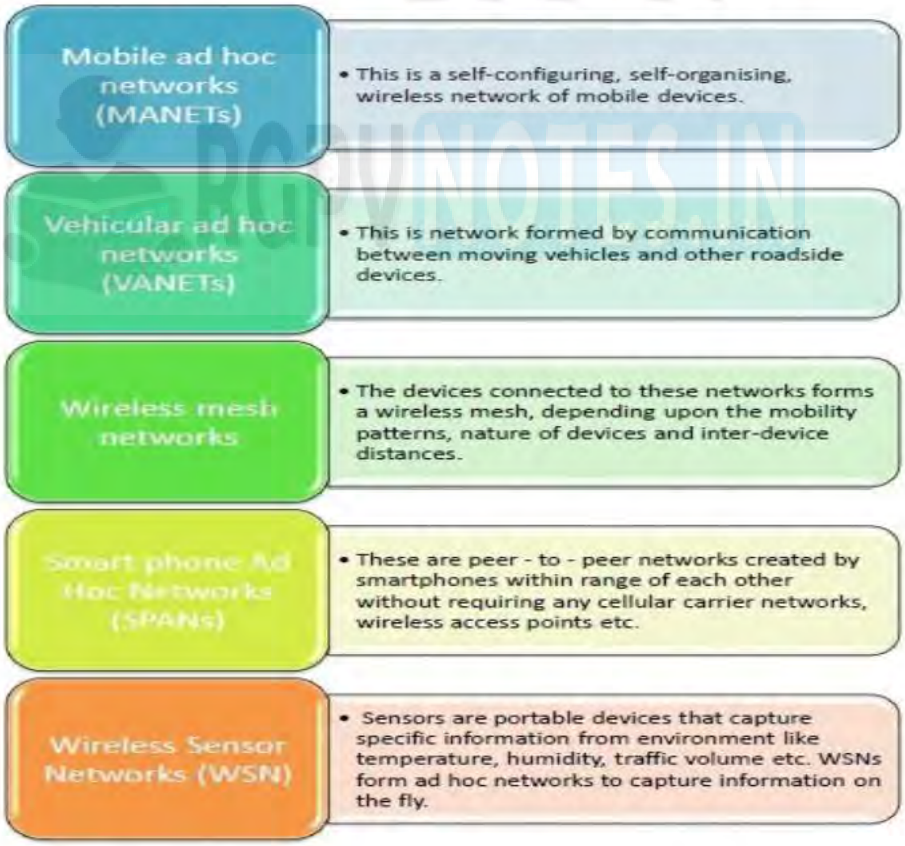


Figure 3.14: ADHOC Network

CLASSIFICATIONS OF AD HOC NETWORKS

Ad hoc networks can be classified into several types depending upon the nature of their applications



Mobile ad hoc networks (MANETs)

- This is a self-configuring, self-organising, wireless network of mobile devices.

Vehicular ad hoc networks (VANETs)

- This is network formed by communication between moving vehicles and other roadside devices.

Wireless mesh networks

- The devices connected to these networks forms a wireless mesh, depending upon the mobility patterns, nature of devices and inter-device distances.

Smart phone Ad Hoc Networks (SPANs)

- These are peer - to - peer networks created by smartphones within range of each other without requiring any cellular carrier networks, wireless access points etc.

Wireless Sensor Networks (WSN)

- Sensors are portable devices that capture specific information from environment like temperature, humidity, traffic volume etc. WSNs form ad hoc networks to capture information on the fly.

Figure 3.15: Classifications of Ad Hoc Networks

TRADITIONAL IP ROUTING

Routing is the primary function of IP. IP datagram's are processed and forwarded by routers which relay traffic through paths set up by various routing protocols. Routing in today's fixed networks is based on network aggregation combined with best matching. TCP/IP hosts use a routing table to maintain knowledge about other IP networks and IP hosts. Networks are identified by using an IP address and a subnet mask, and routes to single hosts are rarely set up. When a packet is to be forwarded, the routing table is consulted and the packet is transmitted on the interface registered with a route containing the best match for the destination. If no network matches are found, a default route is used if one exists.

When configuring a network interface with an IP address, a route to the network the address is a member of is usually registered on the interface automatically. This route is not set up with a gateway (the next hop along the path to the host) since hosts with addresses within this network are assumed to be reachable directly from this interface. This shows that the traditional IP routing maintains an idea of all hosts within the same subnet being on the same link. This means that all hosts in a subnet are available on a single one-hop network segment, typically via routers or switches.

When working on wireless multi-hop networks this is not the case. One needs to redefine the idea of nodes being available ``on the link''. In MANETs nodes routes traffic by retransmitting packets on the interface it arrived. This approach breaks with the wired ``on-link'' way of thinking.

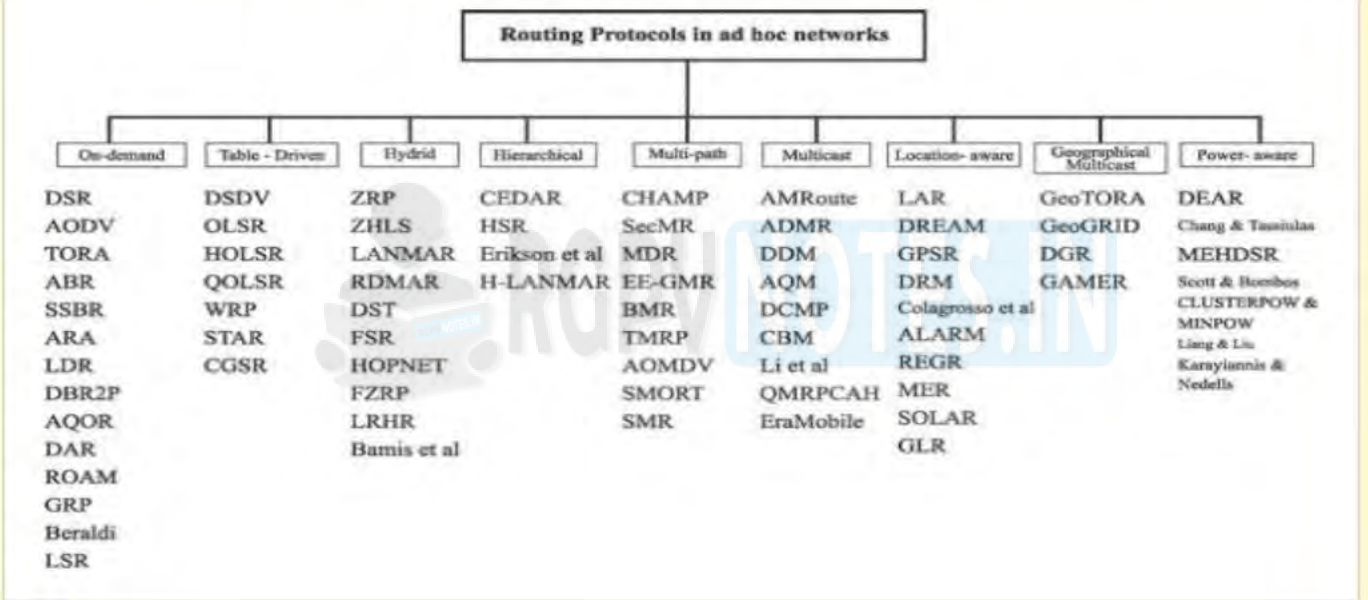
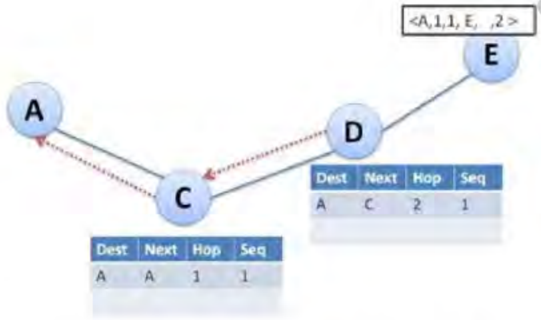


Figure 3.16: Routing Protocols of Ad Hoc Networks

AODV (Ad hoc On-Demand Distance Vector (AODV) Routing): AODV enables "dynamic, self-starting, multi-hop routing between mobile nodes wishing to establish and maintain an ad hoc network. AODV allows for the construction of routes to specific destinations and does not require that nodes keep these routes when they are not in active communication. AODV avoids the "counting to infinity" problem by using destination sequence numbers. This makes AODV loop free. AODV defines 3 message types–

- Route Requests (RREQs): RREQ messages are used to initiate the route finding process.
- Route Replies (RREPs): RREP messages are used to finalize the routes.
- Route Errors (RERRs): RERR messages are used to notify the network of a link breakage in an active route.

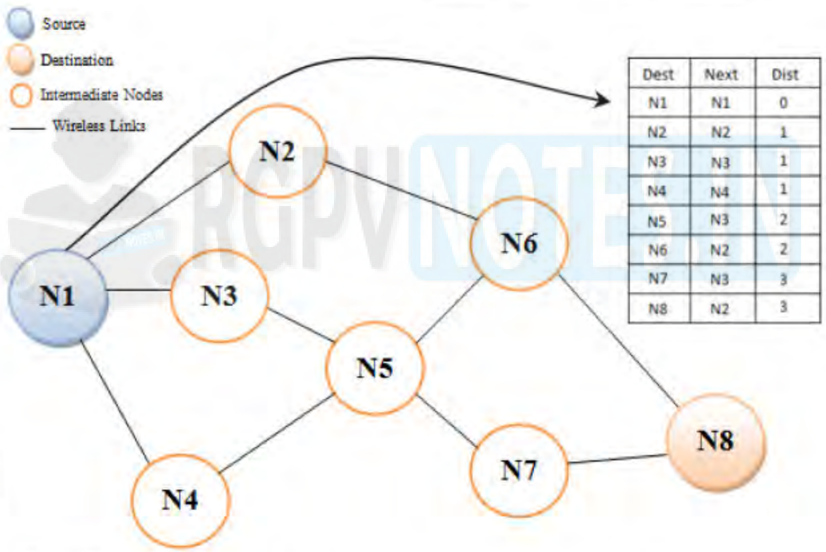


Dest	Next	Hop	Seq
A	C	2	1

Dest	Next	Hop	Seq
A	A	1	1

Figure 3.17: AODV Routing Protocol

Destination Sequenced Distance Vector (DSDV) DSDV is one of the most widely known proactive or table-driven routing protocols for MANETs. The routing algorithm of DSDV is depended on the numeral of hops to arrive at the destination node. To transmit the data packets among the nodes in the network, DSDV protocol utilizing routing tables which are stored in every node. DSDV protocol has three major characteristics which are: decreasing the high routing overhead, solve the “count to infinity” problem and avert the loops. Each mobile node contains a table of routing information which includes all the routes to the destinations and another information.



Dest	Next	Dist
N1	N1	0
N2	N2	1
N3	N3	1
N4	N4	1
N5	N3	2
N6	N2	2
N7	N3	3
N8	N2	3

Figure 3.18: DSDV Routing Protocol

Dynamic Source Routing (DSR): DSR is a reactive or on-demand routing protocol. This protocol has been designed to reduce the bandwidth wasted via the control packets in wireless networks and that via deleting the periodic table-update messages required in the table-driven approach. In DSR protocol, there is no need for network infrastructure or administration, due to these networks fully self-configured and organized. The source routing is a method which the source packet defines the complete sequence of nodes through which to forward the data packets. The source routing does not need to keep the routing information via the intermediate hops.

Zone Routing Protocol (ZRP): ZRP is a hybrid Wireless Networking routing protocol that uses both proactive and reactive routing protocols when sending information over the network. ZRP was designed to speed up delivery and reduce processing overhead by selecting the most efficient type of protocol to use throughout the route.

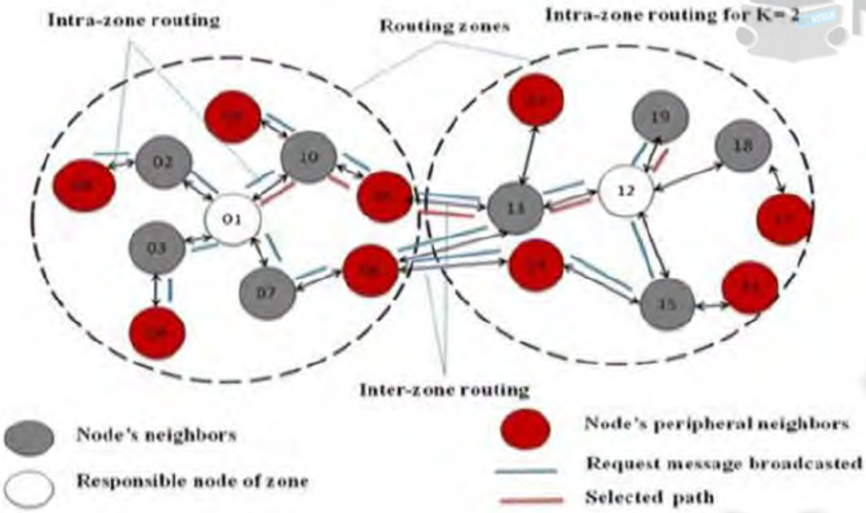


Figure 3.19: Zone Routing Protocol