Unit-I : Ch-1

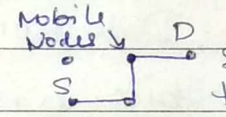
AD HOC AND SENSOR NETWORKS

* INTRODUCTION -

Ad-hoc wireless are defined as the category of wireless networks that are capable of operating without the support of any fixed infrastructure. Hence, they are called infrastructureless networks.

Uses → • Military applications: they establish an adhoc n/w for communication.
• Ad-hoc n/w for communication in remote areas, where infrastructure can't be established
• Home networking: Transfering files b/w two wireless enabled devices.

Features: (Advantages)



Source send data to destination through multiple hops.

- Ad-hoc n/w is a multi-hop network.
- It has a dynamic topology. Since nodes are mobile. Hence, topology changes with mobility of nodes
- Self organising & Self Configuring. (Lower Cost, Nodes don't rely on any hardware & software)

Types:

1) Homogenous Ad-Hoc Networks - Ad-hoc network b/w devices having similar characteristics. Ex: Mobile - Mobile, PC - PC
2) Heterogenous Ad-Hoc Networks - Ad-hoc network b/w devices having dissimilar characteristics. Ex: Mobile - PC - Mobile

More uses / Applications:

1) Crisis Management: Infrastructure is damaged in crisis, at that time adhoc-network can easily be setup.
2) Collaborative Work: Communication among group of people. Also known as collaborative computing.
3) Personal Area Networking: Personal networks such as Bluetooth networking.

* ISSUES IN ADHOC NETWORKS -

- Routing : Wireless devices are mobile, hence, path is not fixed.
- Energy Management : Nodes run out of battery. Transmission of data consumes power.
- Security : No authority to ensure security. It is vulnerable to attacks.
- Quality of Service : Due to mobile nature of nodes, quality large data like video may not be maintained.
- Multicasting : Data transmission in multicasting is difficult as nodes are mobile in nature.
- Medium Access : Lack of infrastructure in MANET, hence, no controlling authority.
- Self Organization : Hence, locating neighbouring nodes is difficult due to this.
- Pricing Scheme : How to charge endusers for internet bandwidth.

* AD-HOC WIRELESS INTERNET -

Adhoc wireless internet extends the service of internet to the end users over an adhoc wireless network.

Applications :

- Wireless mesh network.
- Temporary internet service provision.
- Broadband Internet in rural areas

ISSUES : Same as Adhoc Networks (See Above)

Unit-I : Ch-2

MAC PROTOCOLS FOR ADHOC N/W

* INTRODUCTION-

- MAC (Medium Access Control) Protocol is a set of rules to allow efficient use of a shared medium by multiple users.
- Since, node in ad-hoc wireless network share common broadcast radio channel as broadcast spectrum is limited,
- Ad-hoc wireless networks need to address issues like Mobility, Bandwidth availability, Energy constraints.
- MAC Protocol is concerned with per link communication. (Node to Node)

Need of new protocols in MANETs-

- Lack of centralized protocol.
- Dynamic topology
- Resource contraints (Ex: Energy)
- Not reliable as wired communication.
- Limited bandwidth.

* ISSUES IN DESIGNING MAC PROTOCOL FOR AD-HOC WIRELESS NETWORKS-

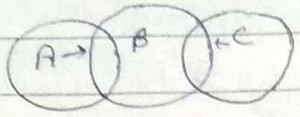
MAC protocol must be designed in such a way that the limited bandwidth is utilized in efficient manner.

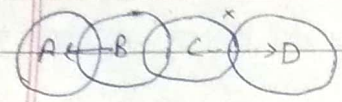
- Bandwidth Efficiency:
  - Efficiently utilize bandwidth.
  - Minimal control overhead.

- Quality of Service Support:
  - Should have resource reservation mechanism.

- Mobility of Nodes:
  - Being wireless, every node is mobile. Hence, dynamic topology.
  - Protocol must be there to handle such topology.

- Synchronization:
  - There must be synchronization b/w nodes in network.
  - Synchronisation is important for Bandwidth reservation by nodes.

- Hidden & Exposed Terminal Problem:
  - 

HIDDEN TERMINALS
Since A is not in range of C & C is not in range of A, they both don't know about each other's state. If they both send packet simultaneously to B, there might be a chance of collision at B. This is Hidden Terminal Problem.
  - 

EXPOSED TERMINAL
In this, B is transmitting data to A. Due to carrier sence, C is prevented to send any data as it may interfere with B's transmission. Even though D can receive from C without any interference (as it is out of range from B), C is not able to transmit any data. This is exposed terminal problem.
  - Hence, these two problems solution must be present in designing MAC protocol.

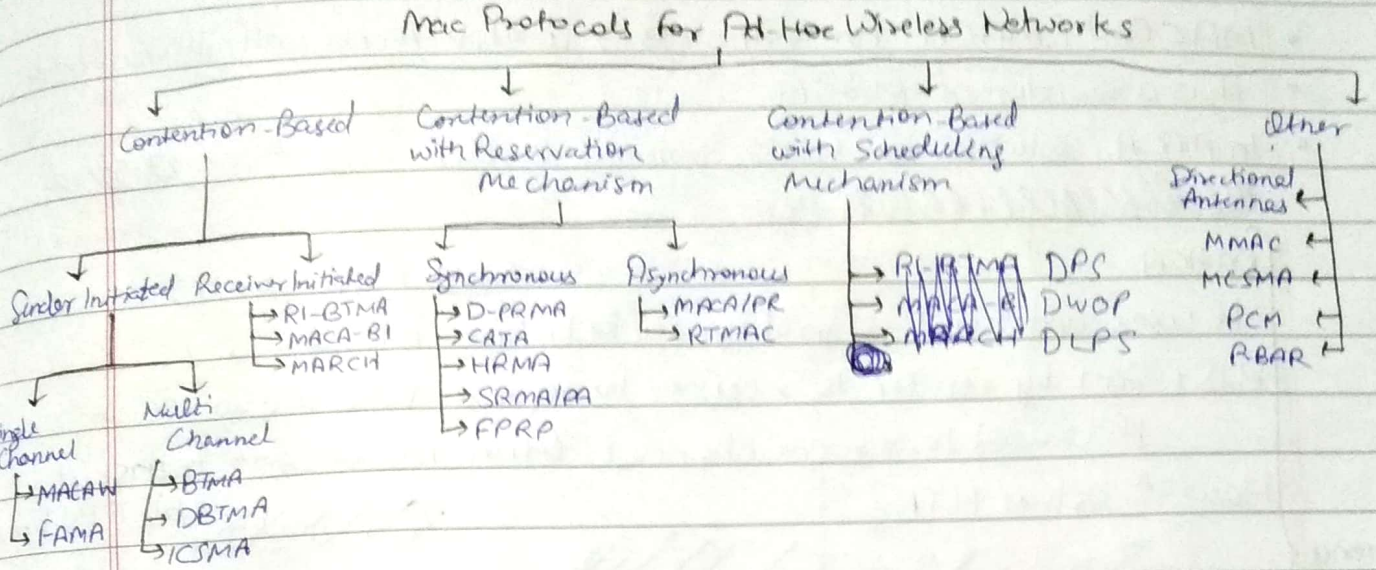
- Error prone shared Broadcast Channel:
  - MAC protocol should grant channel access to nodes in such a manner that collisions are minimized.
  - Nodes must be distributed (scheduled in) fashion for gaining access to channel.

* DESIGN GOALS OF MAC PROTOCOL –

following are the goals to be met while designing MAC Protocol:

- The available bandwidth must be utilized efficiently.
- Must provide QoS: data must be transmitted successfully.
- Operation of protocol should be distributed.
- Protocol must be scalable to large network (as additional nodes may be added).
- Protocol must provide time synchronization among nodes.
- Protocol should have power control mechanism.
- Protocol should minimize the effects of hidden & exposed terminal problem.
- Protocol should ensure fair allocation of bandwidth to nodes.
- Protocol should use directional antennas which provide reduced interferen

* Classification of MAC Protocol-



- **Contention Based Protocol**- It contends (or competes) with its neighbouring nodes for access to shared channel. Hence, it can't provide QoS.
  - **Sender Initiated**: Packet transmission are initiated by sender node.
    - → Single Channel: Node that wins competition (contention) to the channel makes use of entire bandwidth.
    - → Multi Channel: Available bandwidth is divided into multiple channels.
  - **Receiver Initiated**: Receiver node initiate the contention resolution protocol.

- **Contention Based with Reservation Mechanism**- Protocols have mechanism for reserving bandwidth. These can provide QoS.
  - **Synchronous**: It requires time synchronization among all nodes. Global Time synchronization is difficult to achieve.
  - **Asynchronous**: They use relative time information for effecting reservations.

- **Contention Based with Scheduling Mechanism**-
  - Node scheduling is done such that all nodes are treated fairly & no node is starved of bandwidth.
  - Scheduling based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.

* CONTENTION BASED PROTOCOL –

- MACAW (MACA for Wireless) [Multiple Access with Collision Avoidance]
- It is a revision of MACA.
- In MACA, solution for Hidden Terminal Problem uses there [redacted]

MACA

Request To Send Clear To Send

It uses additional signaling packets (i.e. RTS & CTS)

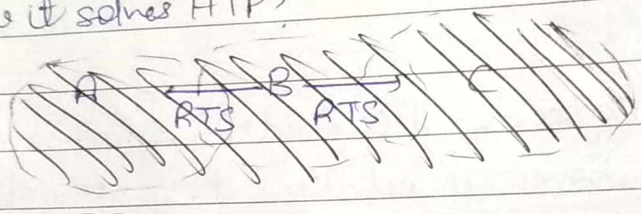
RTS: Sent by sender to receiver to request data transmission.

It is used to reserve channel. Other nodes can't transmit till CTS time.

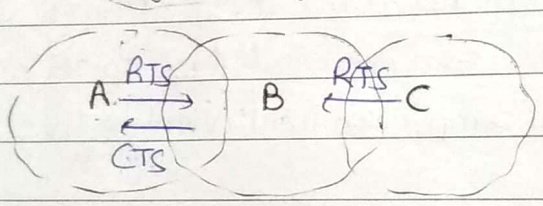
Time taken for data transmission

How it solves HTP?

Reference



DS



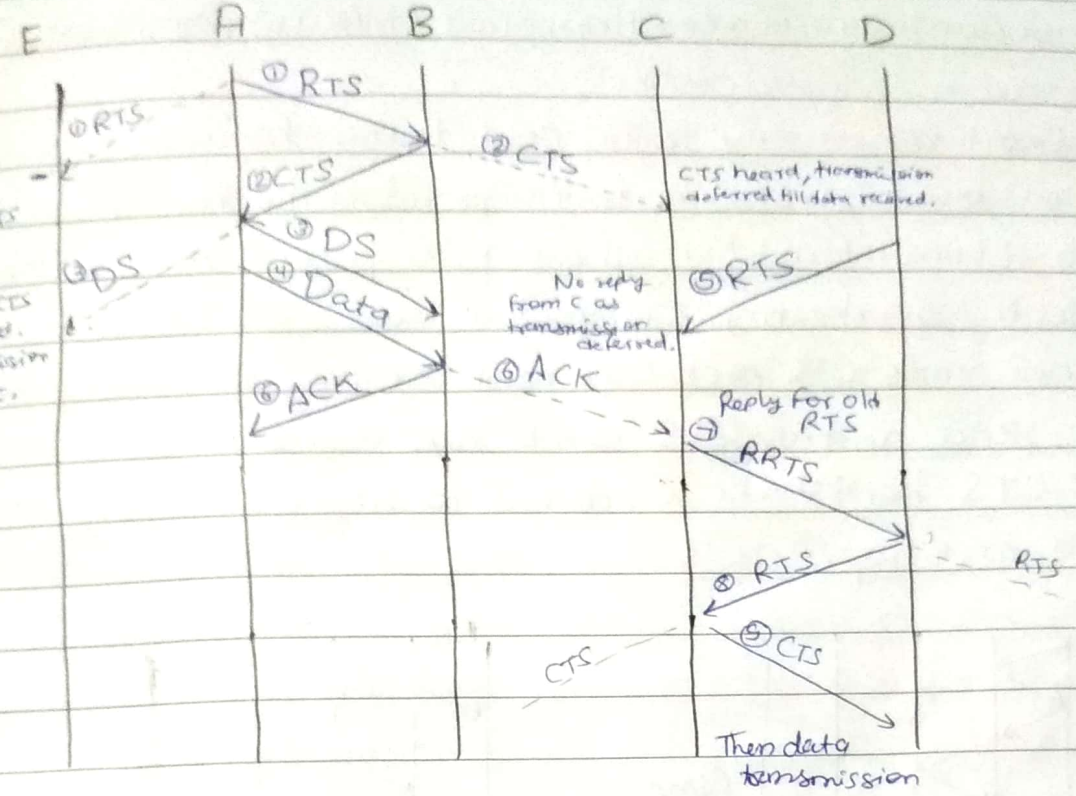
A & C want to transmit to B.

The one whom B sends CTS will be allowed for data transmission only. In this case, A will send data & C will not send.

- In MACAW, sender transmit RTS packet. Receiver replies with CTS. It additionally uses Data Sending (DS) frame which provide information about length of data frame.
- DS indicate successful RTS/CTS handshake.
- Whenever neighbouring station overhear DS, they defer transmission until hearing ACK.

One more feature in MACAW: RRTS ie Request for RTS

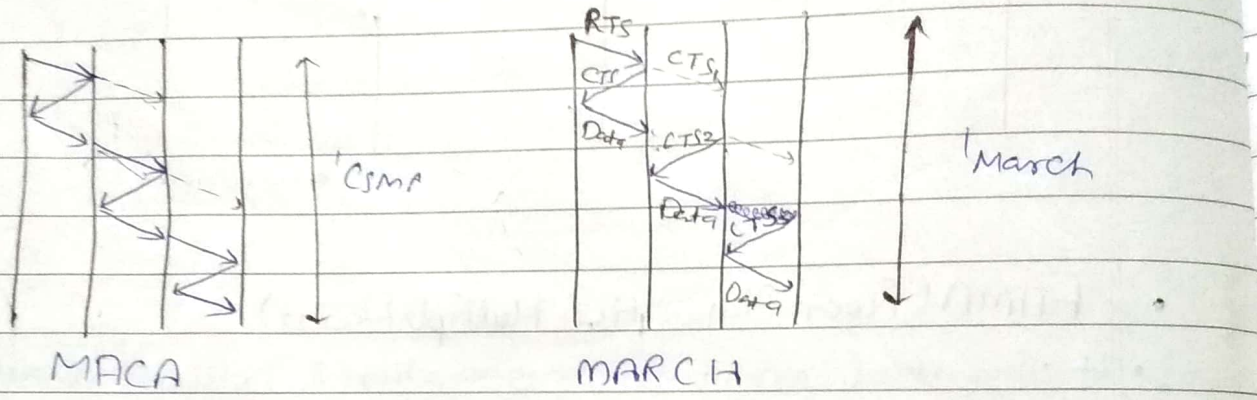
When node C can't reply earlier due to ongoing transmission b/w A & B. sends an RRTS message to D during next contention period. The recepient of RRTS immediately responds with RTS & data transmission is commenced.



- FAMA (Floor Acquisition Multiple Access)
- It consist of carrier sensing operation & collision avoidance b/w the sender & receiver of packet.
- Floor acquisition refers to process of gaining control of channel.
- At any time, only one node is assigned to channel.
- Carrier sensing is done by sender followed by RTS-CTS control packet exchange.
- Hence, it performs as efficiently as MACA.

- MACA-By Invitation Protocol
- It is receiver initiated protocol.
- It reduces number of control packets used in MACA protocol.
- It eliminates the need for RTS packet.
- In this, receiver node initiates data transmission by transmitting ready-to-receive (RTR) packet.
- If sender is ready to transmit, it respond by sending DATA packet.
- Thus, data transmission occurs through 2 way handshake mechanism

- MEDIA ACCESS WITH REDUCED HANDSHAKE (MARCH) PROTOCOL –
  - It is receiver initiated protocol.
  - It doesn't require any traffic prediction mechanism.
  - Exploits broadcast nature of traffic to reduce number of handshakes
  - Node obtains information about data packet arrival at neighbouring nodes by overhearing CTS packet transmitted by them.
  - It then sends CTS packet to neighbour node for relaying data from the node. Hence another RTS can be suppressed.
  - RTS-CTS handshake is reduced to single CTS-only handshake after first hop.



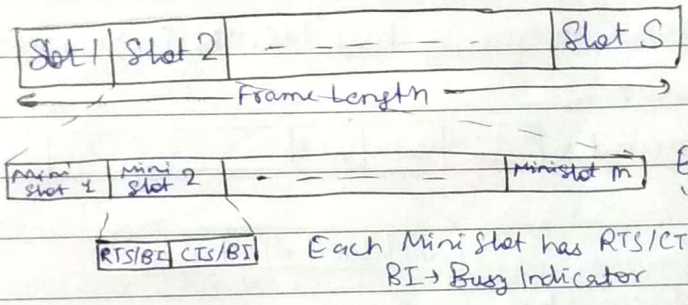
- BUSY TONE MULTIPLE ACCESS (BTMA):
  - Channel is split in two: a data channel for data packet transmission, a control channel used to transmit busy tone signal.
  - Transmitting node senses channel to check whether busy tone is active.
    → If not, it turns on busy tone signal & strarts data transmission.
    → Otherwise it reschedules packet for transmission after some delay.

- DBTMA (Dual Busy Tone Multiple Access): Extension of BTMA
  - A data channel for data packet transmission & control channel for control packet transmission (RTS/CTS packet) & also busy tones.
- RIBTMA (Receiver Initiated BTMA): Two channel → data channel for data packet & control channel for busy tone.
  - Node only transmit data if busy tone absent.

* CONTENTION BASED PROTOCOL WITH RESERVATION MECHANISM -

In contention based protocols, nodes are not guaranteed periodic access to channel (since, they compete). Hence, they can't support real-time traffic.
Contention based protocols with reservation mechanism support such traffic by reserving bandwidth. Hence, they can provide QoS support for real time traffic.

- Distributed Packet Reservation Multiple Access Protocol (DPRMA)
- It extends PRMA in WLAN that can be used in adhoc wireless networks.
- It is TDMA based scheme i.e, channel is divided into equal sized time slots.



- So, nodes compete for mini slots. Once node reserves a slot successfully, remaining (m-1) slots are also alloted to that particular node for transmission. Thats how QoS is maintained.
- RTS is used for reserving slots (mini) & it responds with CTS/BI if reserved successfully.

- Collision avoidance time allocation Protocol (CATA)
- Based on dynamic topology-dependent transmission scheduling.
- Nodes content & reserve time slots by distributed reservation & handshake mechanism.
- It supports unicast, multicast & broadcast transmissions.
- It is based on two principles:

① → Receiver must inform source nodes about reserved slot on which it is receiving packets. Source node must inform destination about interfering in slot.

② → Using NACK for reservation requests; & using control packet transmission at beginning of each slot for distributing slot reservation information to senders.

Frame format: [Slot 1 | Slot 2 | ... | Slot S]

[CMS1 | CMS2 | CMS 3 | CMS 4 | DMS]

Control Mini Slot (CMS) / Data Mini Slot (DMS)

- CMS 1 & CMS 2 inform neighbours of receiving/sending nodes about reservation
- CMS 3 & CMS 4 are used for channel reservation.
- DMS is used for Data Transmission

- Hop Reservation Multiple Access Protocol (HRMA) -
  - It is multichannel MAC protocol based on half-duplex
  - Uses reservation & handshak mechanisms to enable pair of communicating nodes to reserve frequency hop. Hence, it guarantees collision free data transmission.

Frame format: [Synchronisation Slot | Slot 1 | Slot 2 | ... | Slot M]

[SYN | HR | RTS | CTS]

- SYN - Synchronisation
- HR - Hop Reservation
- RTS
- CTS
- Synchronisation Slot → keeps all the slots synchronized.

- Simple Reservation Multiple Access with Priority Assignment (SRMA/PA)
  - Supports integrated services of real-time & non-real time applications
  - Nodes use collision avoidance handshake mechanism & soft reservation mechanisms.

- FPRP (Five Phase Reservation Protocol)
  - Single channel TDMA based broadcast scheduling protocol.
  - Nodes contend to acquise time slots
  - Reservation takes 5 phases: reservation, collision report, reservation confirmation, reservation acknowledgement, packaging & elimination phase.

- MACA with Piggy Backed Reservation (MACA/PR)
  - Provide real time traffic support in multihop wireless networks.
  - Main Components: MAC protocol, Reservation Protocol, QoS Routing Protocol.
  - For real time traffic, each data packet contains information about reservation of next data packet. Hence, this information is piggy backed to it. Each ACK packet also contains this info & thus, neighbours update their information. When sender receives ACK, it makes sure that reservation was successful.

- Real Time Medium Access Control Protocol (RTMAC)
  - Provides bandwidth reservation mechanism for real time traffic.
  - Components in RTMAC:
    - MAC protocol for best effort traffic → Reservation protocol for real time traffic
    - QoS protocol for end to end reservation & release of bandwidth resources.

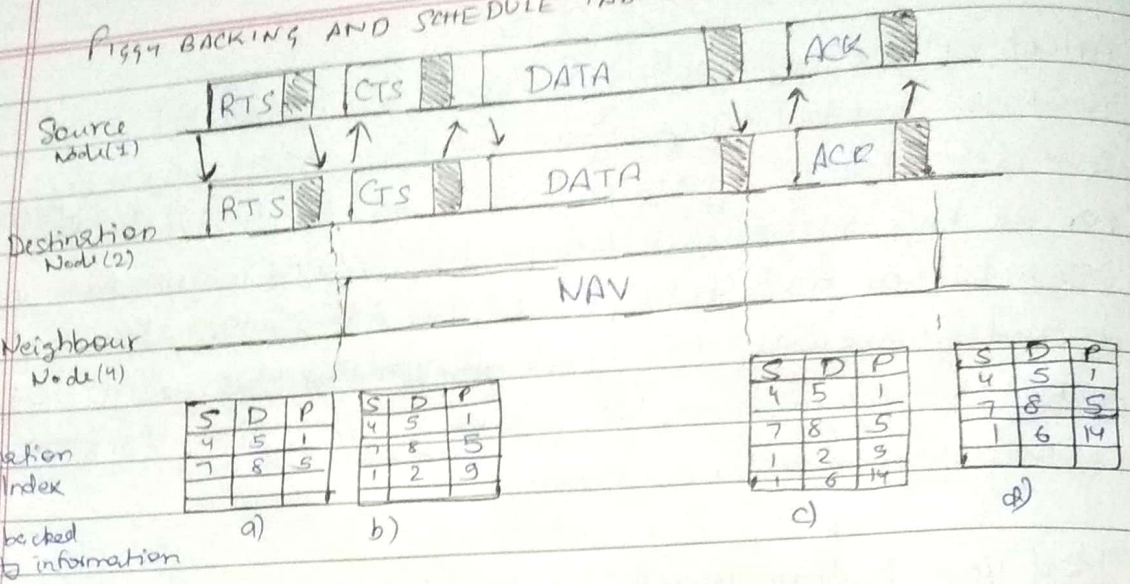
* CONTENTION BASED PROTOCOL WITH SCHEDULING MECHANISMS –

These protocols focus on packet scheduling at nodes & transmission scheduling of nodes. Factors affecting scheduling decisions:
- Delay of packets
- Traffic at nodes
- Battery Power

- DISTRIBUTED PRIORITY SCHEDULING AND MEDIUM ACCESS (DPS) –
  - This technique piggy backs the [redacted] information
  - Head of Line packet is packet with highest priority (low index)
  - RTS, CTS: Carry current packet info.
  - DATA, ACK: - Carry next Head of line info.

A node builds scheduling table by retrieving information from packets being transmitted in its neighbourhood from which it determines rank compared to other nodes.

PIGGY BACKING AND SCHEDULE TABLE UPDATE MECHANISM IN DPS



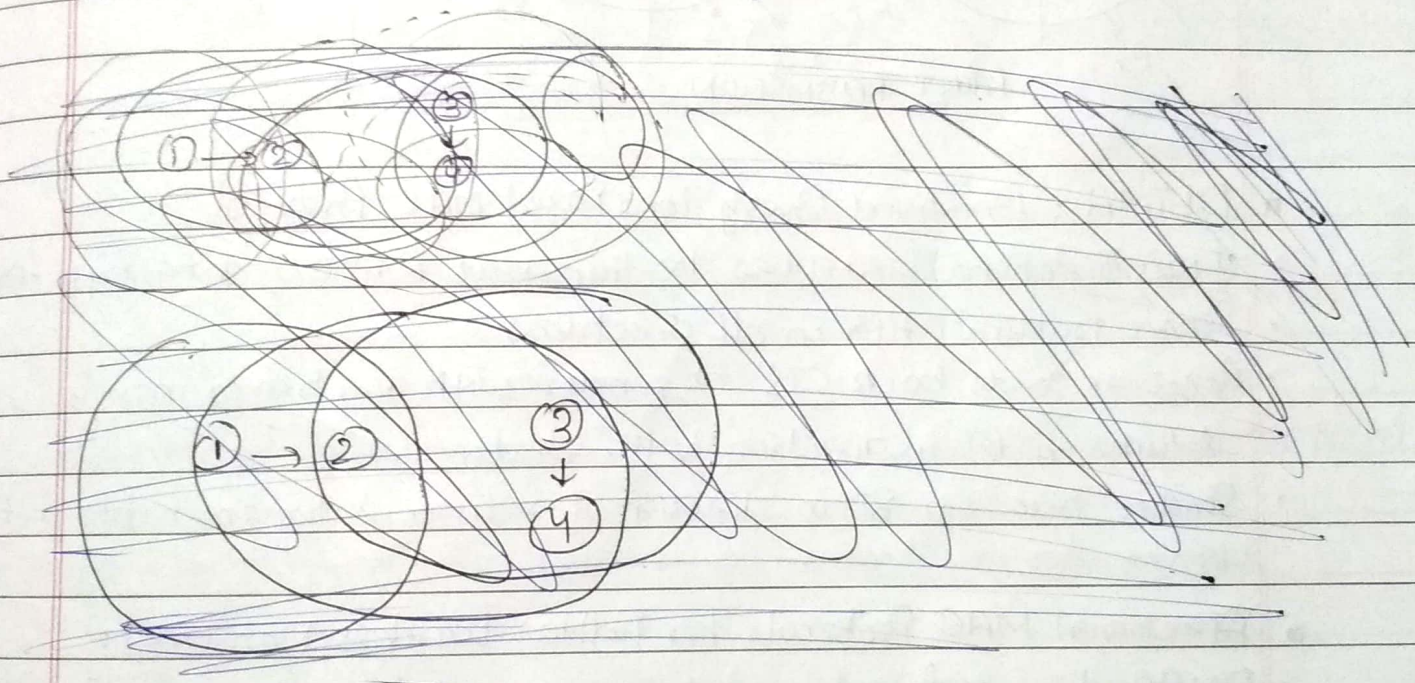
EXPLANATION

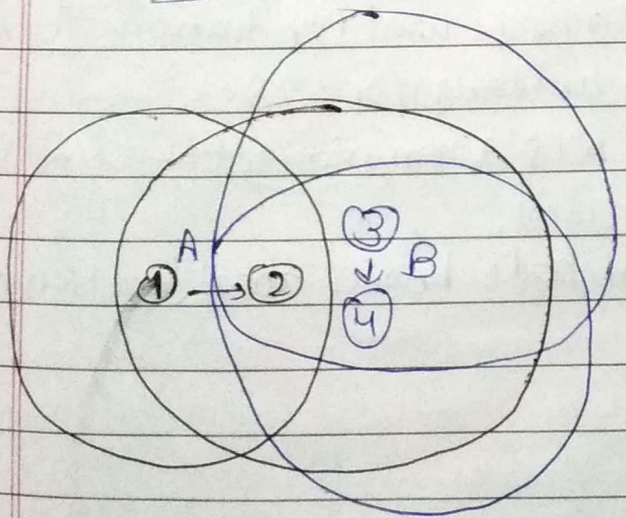
In this, Node 1 transmit data to node 2. It first transmit RTS packet carrying piggy backed information about DATA packet. (with priority index = 9)
Initial state of Scheduling Table of Node 4 is a). Node 4, on hearing this RTS packet, retrieves piggybacked priority information & make corresponding entry in Scheduling Table as shown in b). The destination node 2 responds by sending CTS packet. After receiving CTS packet, source sends DATA packet which contains piggybacked priority info regarding head of line packet at node 1. On hearing this data, Node 4 makes entry for head of line packet of node 1 as in c). Finally, destination sends ACK to source & when this is heard by node 4, it removes entry made for corresponding DATA packet in Scheduling Table. State at the end : d).

- DISTRIBUTED WIRELESS ORDERING PROTOCOL -
  - It is based on DPS scheme
  - It ensures that packets access medium according to the order specified by scheduler such as FIFO, earliest deadline first etc.
  - Similar to DPS, control packets are used in DWOP to piggyback priority information regarding head of line packets of nodes.
  - Each node builds up Scheduling Table ordered according to overheard arrival time.

Problems →

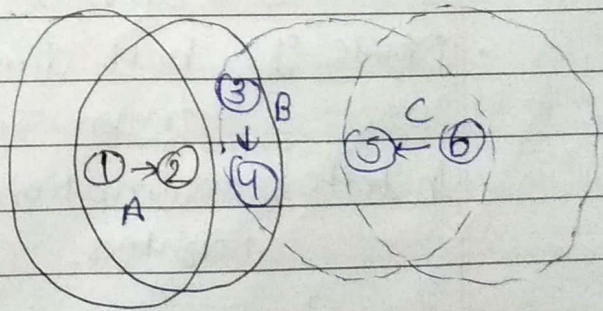
- Information Asymmetry - A transmitting node might not be aware of arrival times of packets queued at other nodes.
  Soln: If receiver finds out that sender is transmitting out of order, an out-of-order notification is piggy backed by receiver on control packets (CTS/RTS)
- Perceived collisions: ACK collide at node, the corresponding entry in ST will never be removed.
  Soln: When node observes that its rank remains fixed while packets whose Piggyback reservation are below priority of its packet are being transmitted, it deletes oldest entry from Scheduling Table.





Black - Coverage of A
Blue - Coverage of B

INFORMATION ASYMMETRY

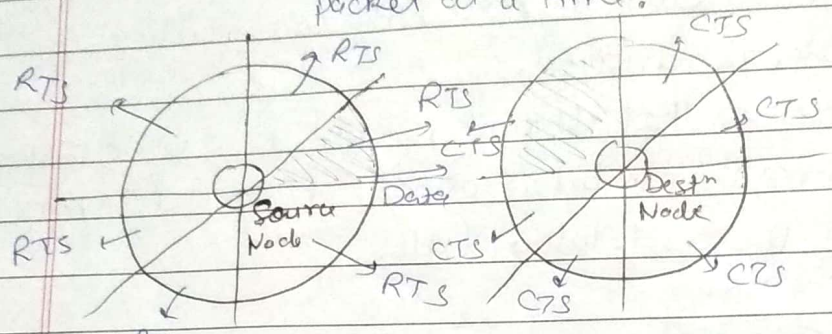


Black - Coverage of A
Blue - Coverage of B C

Perceived Collisions

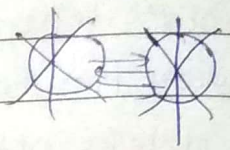
* MAC PROTOCOL USING DIRECTIONAL ANTENNAS -

- Advantages: Reduced signal interference, increased system throughput, improved channel reuse.
- Assumptions: Only one radio tranceiver can transmit/receive one packet at a time.



PACKET TRANSMISSION

TIP: Make like this.



- DBTMA: Directional Busy Tone Based MAC Protocol:
  - It uses directional antennas to transmit RTS, CTS, data, busy tone
  - Sender transmit RTS in all directions
  - Receiver sends back CTS to sender with direction of max power & turns on BT in direction to the sender
  - Sender turns on BT in direction of receiver & transmit data packet.

- Directional MAC Protocols for Adhoc Wireless Networks:
  - DMAC-1, a directional antenna is used for transmitting RTS & omnidirectional antenna for CTS.
  - DMAC-2, both directional RTS & omnidirectional RTS transmission are used.

In both, assumption ⇒ each node knows about location of neighbors.

* OTHER MAC PROTOCOLS -

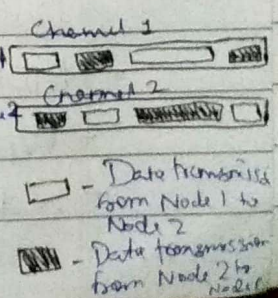
- Multi Channel MAC Protocols: (MMAC)
  - Multiple channel for data transmission.
  - No dedicated control channel.
  - Based on channel usage, can be classified into:
    - → HIGH (High Preference Channel): Channel is selected by current node & is used by node.
    - → MID (Medium Preference Channel): Channel which is free & not being currently used.
    - → LOW (low preference Channel): Already being used in transmission by neighbouring nodes.

- Multi-channel CSMA MAC Protocol (MCSMA)
  - Available bandwidth is divided into several channels.
  - When number of channel is large, each node reserves channel for itself.

- Power Control MAC Protocol (PCM)
  - Allows nodes to vary their transmission power levels on per-packet basis.
  - RTS & CTS are transmitted with maximum power P_{max}.
  - RTS received at receiver with signal P_r.
  - Receiver calculate desired power level $P_{desired}$.

- Receiver Based Autorate Protocol (RBAR)
  - Rate adaptation mechanism is used. (Even at receiver instead of being located at the sender)
  - Rate selection is done during RTS-CTS packet exchange.
  - Rate chosen by sender & receiver are different.

- Interleaved Carrier Sense Multiple Access (ICSMA) -
  - Available bandwidth is split into two equal channels.
  - Handshaking process is interleaved between two channels.

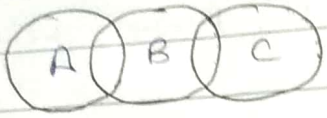


PACKET TRANSMISSION IN ICSMA =>

Unit-II

* INTRODUCTION-

There are lot of protocols which have been developed for Ad-Hoc networks. The routing in MANETs is used to find & maintain routes between nodes in a dynamic topology using minimum resources.
Routing is used in MANETS when a packet has to be transmitted to a destination using intermediate nodes. This also implies that the routing is not required for transmission between nodes that are in range of each other.



So, A to B doesn't require routing
But, A to C requires routing.

* ISSUES IN DESIGNING ROUTING PROTOCOL FOR AD HOC NETWORK-

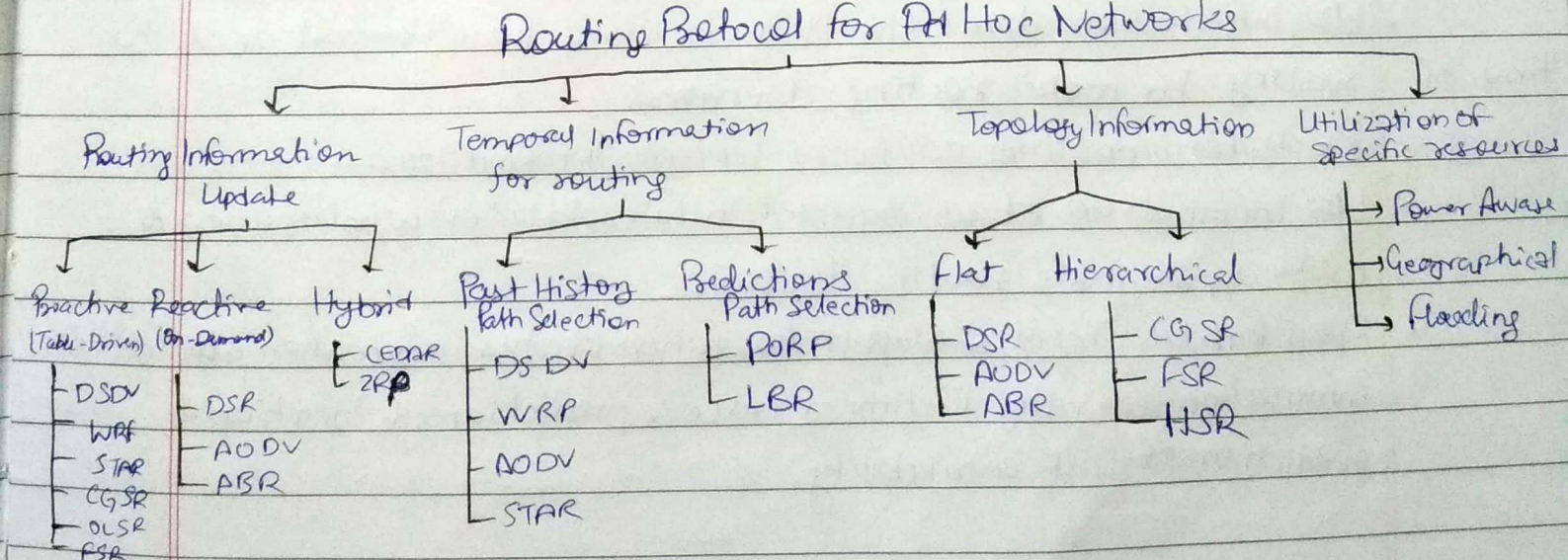
- MOBILITY-
  - Network topology is dynamic due to movement of nodes. Hence, frequent path breakes occur.
  - Routing protocol must perform efficient & effective mobility management.
- BANDWIDTH CONSTRAINT-
  - In wireless networks, the bandwidth is limited as compared to wired networks. Hence, data rates offered are much less.
  - Routing protocol must use bandwidth optimally by keeping overhead low.
- RESOURCE CONTRAINTS-
  - Two essential & limited resources are battery life & processing power.
  - Routing protocol must efficiently manage battery & processing.
  - Devices in MANET are portable, so they have size & weight constraints.
- HIDDEN AND EXPOSED TERMINAL PROBLEM-
  - Explain Hidden & Exposed Terminal as Previously mentioned.
  - Solution for this is- MACA & MACAW (Briefly Explain).

- SECURITY - or controlling
  - No central authority is there in MANET to ensure security.
  - Routing protocols must ensure security of the nodes being involved in transmission.
- ERROR PRONE SHARED BROADCAST CHANNEL -
  - Transmissions in adhoc wireless networks result in collisions of packets.
  - Thus, routing protocol must find path with less congestion.

* CHARACTERISTICS OF ROUTING PROTOCOLS -

- It must be adaptive to frequent topology change caused by mobility.
- Routes computation (or recomputation in case of path breaks) must involve minimum number of nodes.
- Packet collisions must be kept minimum in case nodes broadcast packets for finding paths.
- It must manage the resources of the nodes like battery, processing power, bandwidth efficiently.
- It must ensure security of nodes involved in transmission of packets.
- Must be loop free & provide QoS.

* CLASSIFICATION OF ROUTING PROTOCOLS -



Classification of adhoc wireless networks-

- Based on Routing Information Update Mechanism:

① - PROACTIVE (TABLE-DRIVEN) ROUTING PROTOCOLS :-

- Every node maintains network topology information in the form of routing tables by exchanging routing information.
- Routing information is flooded in the whole network.
- When node requires path to destination, it runs path finding algorithm on topology information it maintains.

② - REACTIVE (ON-DEMAND) ROUTING PROTOCOLS :-

- Do not maintain network topology information.
- Obtains path when required by using connection establishment process.

③ - HYBRID ROUTING PROTOCOLS :-

- Combines both Proactive & Reactive features.
- Nodes within a particular geographical region from a concerned node are said to be within routing zone of given node.
- For routing within this zone, a table-driven approach is used.
- For routing beyond this zone, an on-demand approach is used.

- Based on use of Temporal Information for Routing:

① - ROUTING PROTOCOLS USING PAST TEMPORAL INFORMATION :-

- Use information about the status of links from the past or at the time of routing to make routing decisions.

② - ROUTING PROTOCOLS THAT USE FUTURE TEMPORAL INFORMATION :-

- Use information about expected future status of wireless links to make approximate routing decisions.
- Apart from lifetime of wireless links, future status information also includes information regarding lifetime of node, prediction of location & prediction of link availability.

- Based on routing topology:

① - FLAT TOPOLOGY:-
- It assumes the presence of unique addressing mechanisms for nodes in ad-hoc wireless networks.
- It makes use of flat addressing scheme.

② - HIERARCHICAL TOPOLOGY:-
- Makes use of logical hierarchy in the network & addressing scheme.
- Hierarchy could be based on geographical information or hop distance.

- Based on Utilization of Specific Resources:

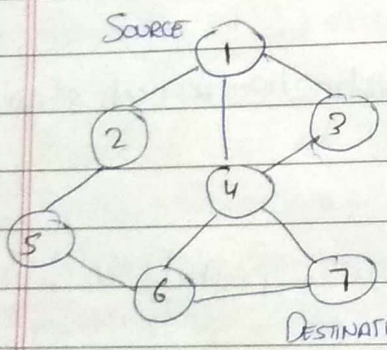
① - POWER AWARE ROUTING:-
- Aims at minimizing consumption of battery in ad-hoc networks.
- Routing decisions are based on minimizing power consumption locally or globally

② - ROUTING USING GEOGRAPHIC INFORMATION:-
- It is routing principle that relies on geographic position information.
- Source sends message to geographical location of destination instead of using network address.
- Hence, it tries to bring message closer to destination in each step using local information.

③ - ROUTING WITH EFFICIENT FLOODING MECHANISMS:-
- They flood the network with RouteRequest packets in order to obtain a path to destination.
- Since flooding of control packets result in wastage of bandwidth & increase in collisions, protocols with efficient flooding mechanisms are used.

* TABLE DRIVEN ROUTING PROTOCOLS - (PROACTIVE)
(Explain Table Driven as previous page)

• Destination Sequenced Distance Vector (DSDV) Routing Protocol:
- It is based on Bellman ford Routing Algorithm.
- Each node's routing table contains list of all available destination & number of hops to reach there.
- It also contains sequence number which is originated by destination node.
- Updates are transmitted immediately (either periodic or event driven).
- Tables are exchanged between neighbours at regular intervals to keep updated view of network topology.
- In table updates, the new sequence number must always be greater than previous one. (Used to avoid loops)
- Table updates are of two types → Incremental Updates & Full Dumps.
It takes single network data packet unit (NDPU) (Only specific entries are sent)
It takes multiple Network Data Packet Units (Full Table is Sent)



ROUTING TABLE FOR NODE 1

Dest^	Next Node	Distance	SeqNo	
2	2	1	22	
3	3	1	28	$Seq_{i+1} > Seq_i$
4	4	1	32	
5	2	2	47	
6	4	2	55	
D→ 7	4	2	67	

Shortest distance is there in routing table ←

So, distance from (1) to (7) is through (4) & it's only 2 hops.

• Wireless Routing Protocol (WRP):
- It is similar to DSDV.
- To counter count to infinity problem, it employs unique method of maintaining information.
- Every node has available route to every destination node in the network.

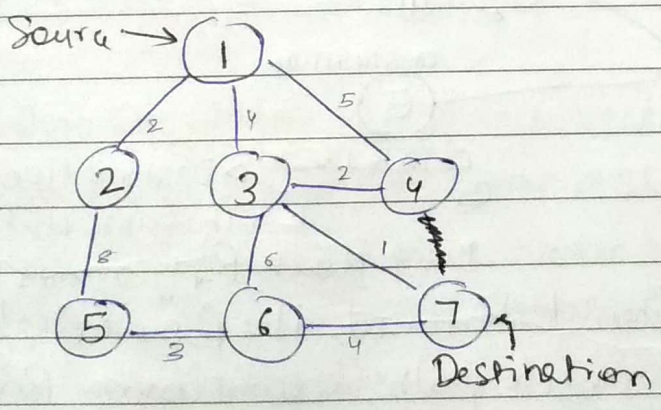
- It differs from DSDV in table maintenance & in update procedures.
- DSDV maintains one topology table while WRP maintain set of tables to maintain information.

→ Tables maintained by a node are -

1) Distance Table (DT): It contains matrix in which each element contains distance & penultimate (almost last) node reported by neighbour for a particular destination.
2) Routing Table (RT): Contains up-to-date views of network for all known destinations.
3) Link Cost Table (LCT): Contains cost of relaying message through each link. The cost of broken link is ∞.
4) Message Retransmission List (MRL): Contains entry for update message that is to be transmitted.

→ Advantages: It involves fewer table updates.

→ Disadvantages: Multiple tables demand larger memory & greater processing power.



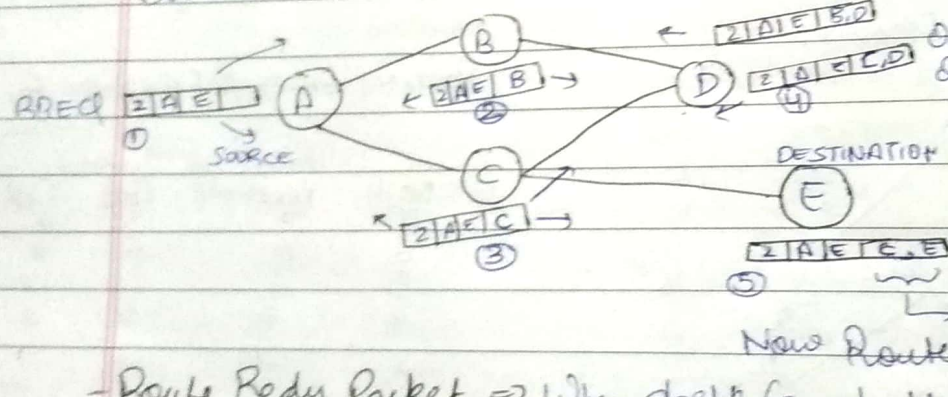
ROUTING ENTRY AT EACH NODE for Destination

Node	(from Source) NextNode	(from Dest.) Pred	Cost
7	7	7	0
6	7	6	4
5	6	6	7
4	3	3	3
3	7	3	1
2	5	6	15
1	3	3	5

* On Demand Routing Protocol (Reactive) -

• Dynamic Source Routing (DSR) Protocol:
- It allows nodes to dynamically discover route from Source to destination
- DSR has two phases:-
① → Route Discovery (Route Request + Route Reply)
② → Route Maintainence

① Route Discovery:
- Route Request Packet ⇒ UniqueID, Source Address, Dest" Addr, Blank List field
(RREQ) [UID | SA | DA | List]
This request packet is broadcasted from source & further nodes broadcast it as well & attach their address in the "list". Hence, multiple copies of same Unique ID are discarded. Packets are broadcasted till destination is found.



Now Route Reply occurs
- Route Reply Packet ⇒ When dest" found, the Route Reply packet (RREP) is sent along reverse path received from RREQ list.
It containing path ⇒ [A → C → E] this is Send to A.
from SA ↳ from List

When RREP is received at Source Node, it sends the data to destination along the path which is included in header of A from RREP ⇒ [A → C → E | DATA] Data is send from A to D.

② Route Maintenance:

- ROUTE CACHE - If a packet has to sent to same destination, the node will not repeat route discovery process again. The routes discovered will be cached by source node & hence, if another packet has to be transmitted to same destination, it'll recover path from cached route. [A→C→E]
- ROUTE ERR (RERR) - If a node in cached route is broken, it will send RERR packet to source through intermediate nodes. Thus, the source will remove that node from cached routes.

If (A) RERR (C) ✕ (E) RERR

Cache [A→C✕E]

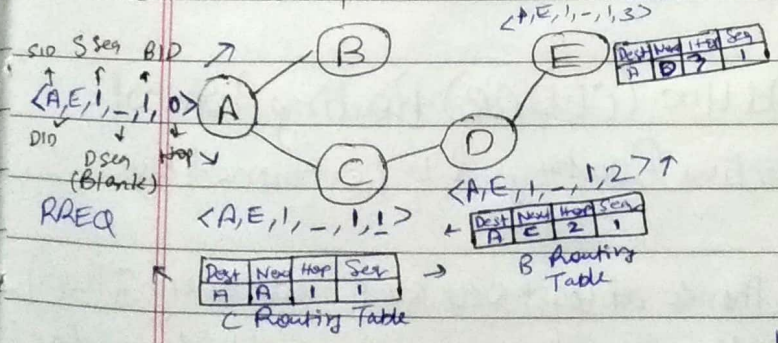
Cache New [A→C]

ADVANTAGE : ① Route established only when required.
② Use of Route Cache reduce control overhead.

DISADVANTAGE : ① Route Maintainence doesn't repair broken link.
② During sending data, it includes Path also. [Path | DATA]
So, if Path is very large, bandwidth may not be efficiently utilized.

- Adhoc On Demand Distance Vector (AODV) Routing Protocol -
  - It overcomes DSR disadvantage i.e, path is included in header while sending data from source to destination.
  - Two phases: ROUTE DISCOVERY AND ROUTE MAINTAINENCE

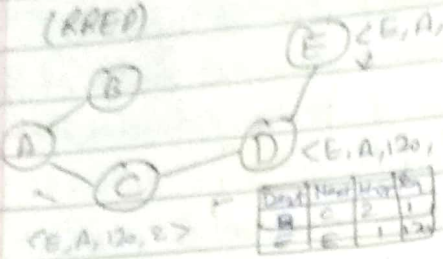
I] ① Route Request (RREQ) => SourceID, DestID, Source Seq, Dest Seq, Broadcast ID, Hop Count



RREQ is broadcasted to neighbouring nodes from source & they are further broadcasted till destination is found.
Meanwhile, all the intermediate nodes to whom RREQ is broadcasted maintain routing table as: [Dest | Next | Hop | Seq]

As RREQ reaches destination, RREP is unicast to source.

I) ② Route Reply - It contains (Sender, Receiver, Dest Seq No, Hop count)
(RREP)



Hence, the RREP is unicasted & intermediate nodes update their routing table as well so as to track path to reach 'E' destination.

As soon RREP reaches source it will send only data i.e, DATA & hence, path information is not included in the header of data.

These two steps were of the phase ROUTE DISCOVERY. I)
Now second phase:

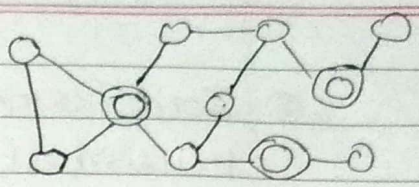
II) ROUTE MAINTENANCE - If a node link is broken, it sends Route Error (RERR) packet to neighbours (broadcast) & they further broadcast & when it reaches 'A', source gets to know that some link is broken.
Hence, the source starts with first phase i.e, Route Discovery again to find appropriate path.

Advantage over DSR → AODV doesn't contain the full path as data packet intermediate nodes store next hop information.

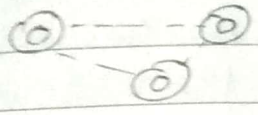
- HYBRID ROUTING PROTOCOLS-

① Core Extraction Distributed Ad Hoc (CEDAR) Routing Protocol -
- Route establishment uses Reactive Routing. & is performed by core nodes.

CONCEPT: Core Extraction. (There's at least one core node every 3 hops)
- Every node picks up a node within one hop from it, as its dominator.
- Core consist of dominator & tunnels. (Tunnels consist of non core nodes)



CEDAR PHASE I ⇒ • find core nodes
• Establish virtual links



——— → Bidirectional Links ○ → Node
- - - → Virtual Links b/w Core Nodes ◎ → Core Node

CEDAR PHASE II → ①• Check local topology ②• Initiate Route Request
③• Core Broad Cast ④• Route Reply ⑤• Core Path

Thus, these core nodes perform reactive routing (i.e, On demand routing).

In case of LINK BREAK →

- The Node after which break occurred:

① → Sends notification of failure ② → begin to find new path to destination
③ → rejects received packets till it finds new path to destination.

- When source node receives notification:

① → it stops transmission ② → It tries to find new route to destination

If new route is found by either of these two nodes, a new path from source to destination is established.

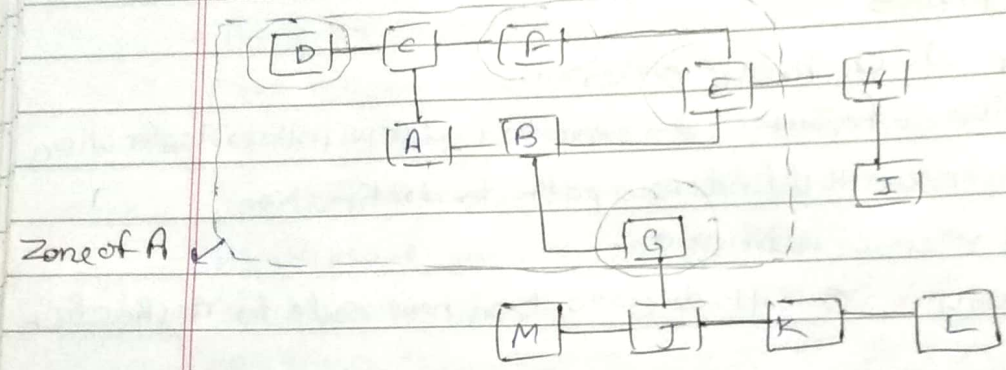
ADVANTAGE- Use of core nodes reduce traffic overhead.
DISADVANTAGE- Core node's movement affects performance.

② ZONE ROUTING PROTOCOL (ZRP) -

- It uses best part of Proactive & Reactive routing protocols.
- Divides the network into zones: (As per zone Radius)
  - ① Intra Zone Routing Protocol (IARP) → The zone within the zone radius from a particular node. (In this → Proactive Routing)
  - ② IERP (Inter Zone Routing Protocol) → The zone outside the zone radius from a node. In this, Reactive Routing.

* Zone Radius → Number of hops from a node to determine zones.
* Peripheral Nodes → Nodes with distance/hop equal to zone Radius.

WORKING:



Source → A
Destination → L
Zone Radius → 2

I) ROUTE ESTABLISHMENT -

- Checks if destination is within zone (Not in Example)
  - ↳ If in zone, proactive protocol is used (Route REQ / Route REP)
  - ↳ If not, node sends route query to peripheral nodes.
    (Route Query to D, F, E, G)
    - ↳ Now, every peripheral node will check for destination in their zone
      (Not in D, F, E, G Zone) Then each will check in their zone
      So, G will not have. It will send to peripheral 'K'
      'K' has in local zone.
      Now K will return requested route. (L-K-G-A)

Loop

IMP → Each node attach their IP address in packet. That's how packets are transmitted back to source.

* LINK BREAK → After node detects link break:
  ① Choses alternative path ② Path update message is sent to sender to inform it about link failure.

ADVANTAGE → Reduce wastage of bandwidth & control overhead.
DISADVANTAGE → large overlapping of routing zones.

* ROUTING PROTOCOL WITH EFFICIENT FLOODING MECHANISM -

① Preferred Link Based Routing (PLBR) Protocol:
- Uses preferred link if a RouteRequest packet is received through strong link.
- Here, a node selects subset of nodes from Neighbours List (NL). This subset is called Preferred List (PL).
- All neighbours receive RREQ packets but only neighbours in PL forwards them.
- Each node also maintains Neighbor's Neighbor Table (NNT).

Preferred Link Computation:

① Neighbor Degree Based Preferred Link (NDPL) Algorithm -
Based on neighbor node's degree. Divides it into reachable/unreachable

② Weight Based Preferred Link (WBPL) Algorithm -
Based on weight given to specific node. Weight based on its neighbors Spatial stability.

RouteRequest Packet ⇒ <SA, DA, SeqNo, Traversed Path, PL, TTL>
↳ Time To Live
It is always broadcasted to neighbors but only the ones in PL can forward it.

ROUTE ESTABLISHMENT:
1) If dest. is in source's NNT, route is established directly. Otherwise source transmit RouteReq packet. (Broadcast)
2) Only PL nodes can forward broadcast.

PATH SELECTION: When multiple RREQ reach dest^n → Best route is selected i.e shortest path, least delay path or most stable path.

* LINK BREAK → Uses next two hop info from NNT to bypass broken link.
* ADVANTAGE → Flooding efficient protocol reduces collisions & control overhead.
* DISADVANTAGE → PLBR & WBPL are computationally complex.
NDPL

② * Optimized Link State Routing (OLSR) Protocol-

- This is based on Link State Routing.
- In LSR, packets are flooded inefficiently which consumes more bandwidth & high power.
- OLSR makes efficient use of LSR & uses Multipoint Relaying (MPR) & mechanism for packet forwarding.
- Each node decides which of its neighbors can flood packets. These nodes are called MPR (Multi Point Relay).
- MPR is subset of node's neighbor & only MPR can retransmit packets & not other nodes.
- MPR are generally 1-hop neighbour which have access to all two hop neighbors. → $N_2(u)$ → $N_1(u)$
- There are two types of links in which nodes may exist
  - ↳ Symmytrical (Bidirectional)
  - ↳ Asymmetrical (Unidirectional)
- OLSR have [redacted] packets:

① HELLO Packets: Each node broadcasts HELLO messages to 1-hop neighbors. It contains info about its neighbors & their link status.

When node receives HELLO message, it constructs its MPR Selector Table.

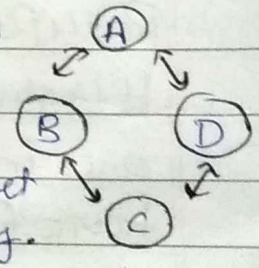
Through this table, MPR nodes are selected.

IMP⇒ Selects nodes in $N_1(u)$ which cover isolated points of $N_2(u)$

Where 'u' is a node.

$N_1(u)$ → 1-hop neighborhood of u

$N_2(u)$ → 2-hop neighborhood of u.



If A selects B as MPR, so C will receive packet from B only. Hence, no duplicates.

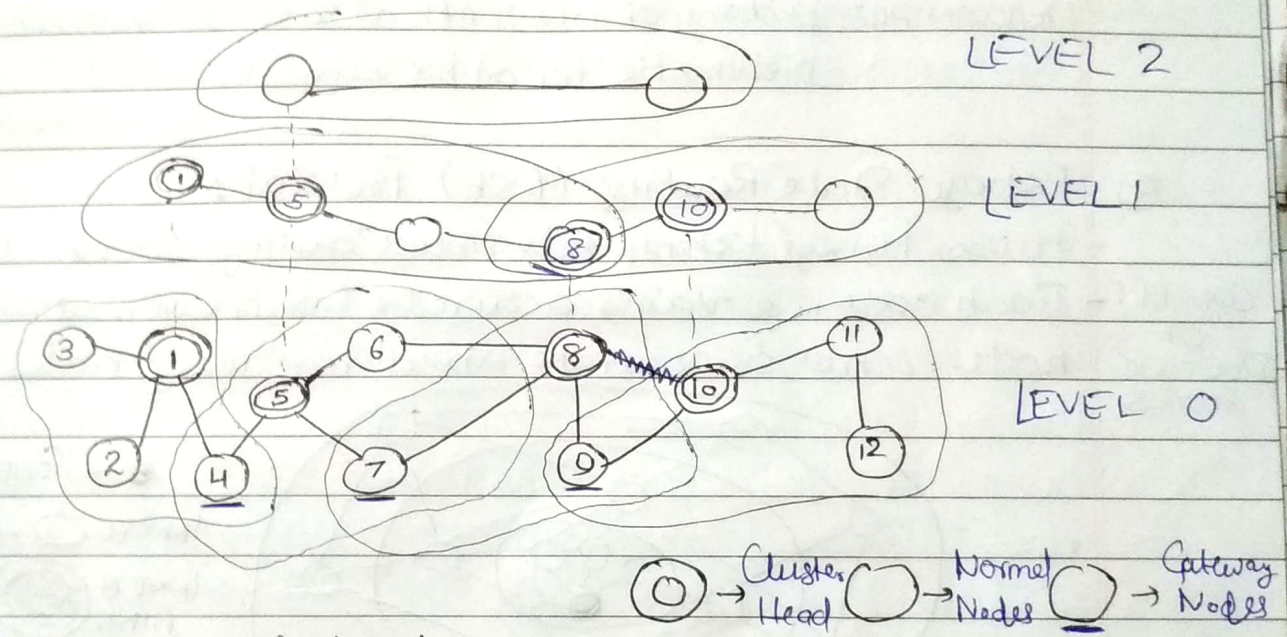
ADVANTAGES - Reduced number of broadcast, Minimal Control Overhead.

DISADVANTAGES - Overlapping MPR sets.

* HIERARCHICAL ROUTING PROTOCOLS-

① Hierarchical State Routing (HSR) Protocol:

- It is a Distributed Multi Level Hierarchical Routing Protocol.
- HSR defines different levels of clusters.
- Each cluster has its leader. Clusters are organized in levels
  → Physical - b/w nodes having one hop links between them.
  → Logical - based on certain relations



Nodes are classified into:

① Cluster Heads - Node elected as cluster head or leader. (Path b/w 2 cluster leaders is called virtual link)
② Gateway Nodes - Belong to 2 or more clusters.
③ Normal Nodes - Belong to single cluster.

PROPERTIES -

① → Cluster Heads at Level 0 → • Schedule packets for transmission
• Exchange routing information
② → Gateway Nodes → • forward packets b/w different clusters
③ → Every node maintains status of link with its neighbors
④ → Path b/w 2 cluster head involves multiple links called virtual link.
Virtual Link → Head - Gateway - Head - Gateway etc.

Ex: Path b/w L1-1 to L1-10 ⇒ (1 → 4 → 5 → 7 → 8 → 9 → 10)
H G H G H G H

⑤ → HSR address is <HeadID - NodeID>
Ex: HSR of Node 12 is → <10-12>

⑥ → Every node's hierarchical address is stored in HSR table & it indicates location in hierarchy.

ROUTE ESTABLISHMENT:

① Forwards packet to highest node in hierarchy of source.
② Sends it to highest node in hierarchy of destination.
③ Packet is forwarded from this node to the destination node.

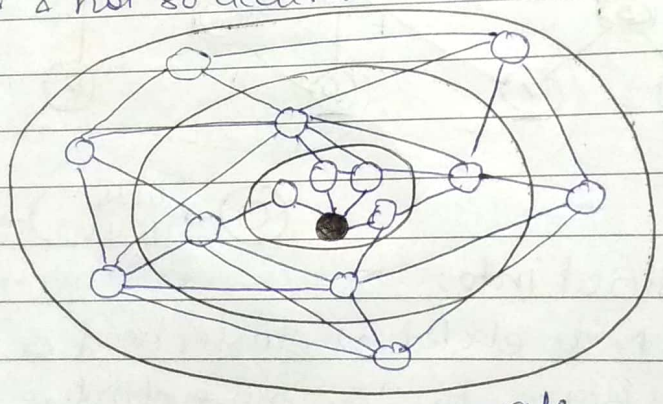
ADVANTAGE: Using hierarchy information, it reduces routing table size.
DISADVANTAGE: Exchange of info. with all levels of hierarchy makes it problematic for ad hoc networks.

② Fisheye State Routing (FSR) Protocol:

- It uses fisheye technique to reduce routing overhead.

CONCEPT OF ROUTING SCOPES

- Each node maintains accurate information about nearby nodes & not so accurate about far away nodes.



- So, central node has most accurate information about INNER ○.
- Nodes exchange topology information only with their neighbors.
- The exchange in smaller scopes are more frequent than in larger. Hence, info. about nearby nodes are more precise than farther.
- As the packet approaches destination, the route becomes more & more accurate.

ADVANTAGE - Reduces bandwidth consumption as link state packets are shared only with neighbors. Routing overhead is also reduced.
DISADVANTAGE - Very poor performance in small Adhoc networks

* POWER AWARE ROUTING PROTOCOLS -

Metrics taken into account for route selection procedure:

- Minimal energy consumption per packet
  - This aims at minimizing power consumed by packet in traversing from source node to destination node.
- Maximize Network Connectivity
  - It attempts to balance routing load among nodes in the network.
- Maximum variance in Node power levels
  - It proposes to distribute the load among all nodes in the network so that power consumption remains uniform across them.
- Minimum Cost per Packet
  - Cost as a function of battery charge. A node's cost decrease with increase in battery charge (energy) or vice versa.
- Minimize Maximum Node Cost
  - It minimize maximum cost per node for a packet after a specified period.

→ Power Aware Source Routing (PSR)-

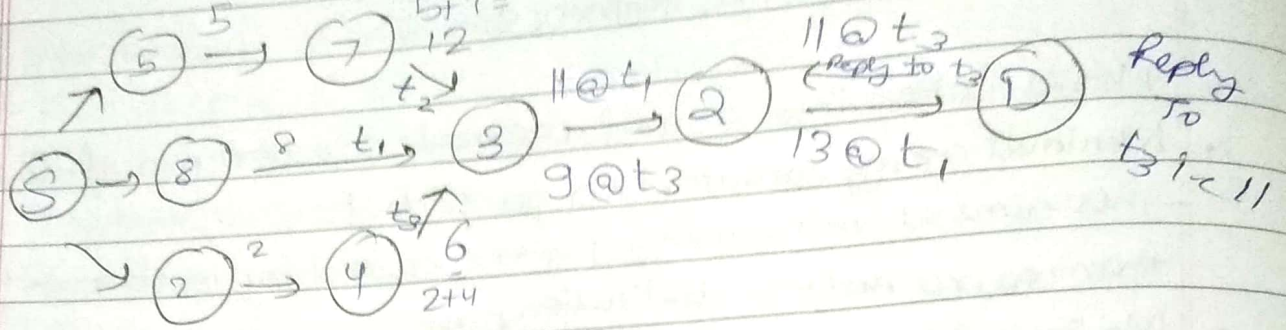
- It is reactive (on-demand protocol based on DSR).
- The cost function of Route Π at Time t is $C(\Pi, t)$.
- The cost function takes into account both transmission Power & remaining battery power.

ROUTE DISCOVERY:

→ RREQ broadcasted by source.
→ Intermediate nodes having cache can reply to RREQ.
→ If there's no cache, intermediate node:
- Starts Timer • Keeps path cost in header as Min-Cost • Adds its own cost to path cost & broadcast

→ On receiving duplicate RREQ, intermediate node rebroadcasts only if:
- Timer for RREQ has not expired • New path cost is less than Min-Cost.

→ Destn waits for specific time after first RREQ is received.
→ It then replies to best path & ignores others.
→ Path cost is added to reply & cached by all nodes that hear reply.



ROUTE DISCOVERY IN DSR.

Unit-II : Ch-2

* INTRODUCTION:

Transport Layer

- TCP (Transmission Control Protocol) objectives includes the setting up of:
  - → End to End Connection
  - → End to End Delivery of Data Packets
  - → Flow Control
  - → Congestion Control
- Transport Layer Protocols:
  - → TCP (Transmission Control Protocol): Reliable, Connection Oriented
  - → UDP (User Datagram Protocol): Unreliable, Connection less Protocol.
- These traditional wired transport layer protocols are not suitable for adhoc wireless networks.

* ISSUES IN DESIGNING TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS -

- Induced Traffic:
  - It refers to traffic at any given link due to the traffic through neighbouring links.
  - it is due to broadcast nature of channel which affects the throughput achieved by Transport Layer Protocol.

- Induced Throughput Unfairness:
  - it refers to throughput unfairness at transport layer due to throughput unfairness existing at lower layers such as N/W & MAC layer.
  - transport layer should consider these in order to provide fair share of throughput.

- Separation of congestion control, reliability & flow control:
  - transport layer protocol can provide performance if end to end reliability, flow control & congestion control are handled separately.

- Power & Bandwidth Issues:
  - Nodes in MANETs face resource constraints of most important resources i.e power & bandwidth.
  - The performance of Transport layer protocol is significantly affected by these resource constraints.

- Misinterpretation of Congestion:
  - Interpretation of congestion in traditional n/w is not suitable for MANET.
  - This is because of high error rates of wireless channel, hidden terminal problem, path breaks, packet collisions in MANETs.

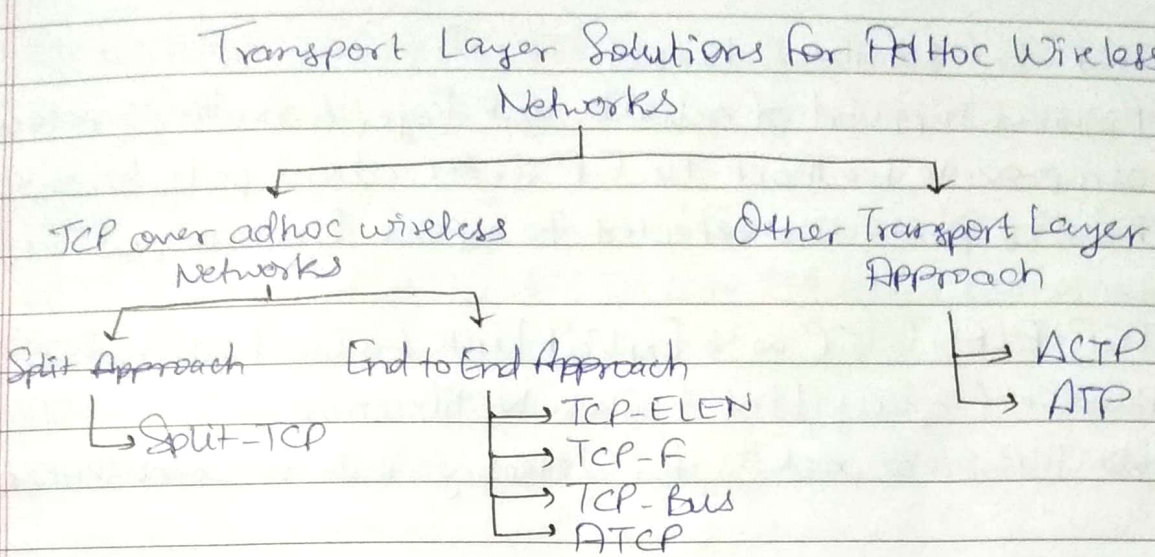
- Completely Decoupled Transport Layer:
  - Interaction with the lower layers is a challenge for Transport Layer Protocol.
  - Interaction is necessary so as to adapt to changing network environment.

- Dynamic Topology:
  - Rapidly changing network topology due to mobility of nodes.
  - It leads to frequent path breaks, partitioning & re-emerging of networks & hence, affects performance of Transport Layer.

* DESIGN GOALS FOR TRANSPORT LAYER IN AD-HOC WIRELESS NETWORKS -

- Protocol should maximize throughput per connection.
- It should provide throughput fairness across contending flows.
- It should minimize connection setup & connection maintenance overheads.
- Protocol should have mechanisms for congestion control & flow control in the network.
- It should provide both reliable & unreliable connections.
- Protocol should be able to adapt to the dynamic topology.
- Bandwidth must be used efficiently.
- Protocol should be aware of resource constraints such as battery power & bandwidth.
- It should have well defined cross layer interaction framework.
- It should make use of information from lower layers.
- It should maintain end to end semantics.

* CLASSIFICATION OF TRANSPORT LAYER SOLUTIONS -



* TCP Over Adhoc Wireless Networks -

. Why does TCP does not perform well in Adhoc Wireless Networks:

→ Misinterpretation of Packet Loss:- TCP was designed for wired n/w where packet loss is attributed to network congestion. So, if packet loss is detected, sender assumes congestion in the n/w & invokes Congestion Control Algorithm.

→ Frequent Path Breaks:- There are frequent topology changes, hence dynamic topology due to mobility of nodes in the network. Hence, route to a destination need to be recomputed very often.

→ Effect of Path Length:- TCP throughput degrades rapidly with increase in path length.

→ Misinterpretation of Congestion Window:- TCP consider consider congestion window as measure of rate of transmission acceptable to network & receiver. In adhoc wireless n/w, congestion control mechanism is invoked when path break occurs.

→ Network Partitioning & Remerging:- Due to dynamic topology.

- PROTOCOLS IN TCP OVER AD HOC NETWORKS -

- TCP-F (Feedback based TCP)
  → Requires support of reliable link layer & routing protocol that can provide feedback to TCP sender about path breaks.
  → Routing protocol is expected to repair broken path.

- TCP-ELFN (TCP with Explicit Link Failure Notification)
  → Handle Explicit Link Failure Notification.
  → Use TCP probe packets for detecting route reestablishment.

- TCP-BuS (TCP with Buffering Capability & Sequence Information)
  → Use feedback information from intermediate node on detecting path break
  → Use LQ (Localized Query) & REPLY to find partial path.
  → On detecting path breaks, intermediate node originates ERDN (Explicit Route Disconnection Notification) message.

- ATCP (Ad Hoc TCP)
  → Use network layer feedback to make TCP sender aware of status of network path.
  → Based of info. received from intermediate nodes, TCP sender changes its state to persist state, congestion control state or retransmit state.

- Split TCP
  → Provides solution to channel fairness problem by splitting transport layer objectives into congestion control & end-to-end reliability.
  → Splits long TCP connection into short concatenated TCP connection.

OTHER TRANSPORT LAYER PROTOCOLS -

- ACTP (Application Controlled Transport Protocol)
  → It assigns responsibility of ensuring reliability to application layer.
  → ACTP is b/w TCP & UDP where TCP experience low performance with high reliability & UDP provides better performance with high packet loss.
  ADV → Scalable for large nlw. No congestion window.
  DISADV → Not compatible with TCP. May Lead to heavy congestion.

- ATP (Adhoc Transport Protocol)
  → provides coordination among multiple layers & assisted congestion control.
  → it uses information from lower layers for:
  - Estimation of initial transmission rate
  - Detection, Avoidance & Control of Congestion
  - Detection of path breaks.

  ADV → Improved performance
  DISADV → Lacks interoperability with TCP.

* SECURITY IN ADHOC WIRELESS NETWORKS:

• NETWORK SECURITY REQUIREMENTS-

→ Confidentiality: The data sent by sender (source node) must be accessible only to the intended receiver (destⁿ node). It is concerned with ensuring that data is not exposed to unauthorized users.

→ Integrity: The data sent by source node should reach the destination node as it was sent. Hence, unauthorized users should not be able to modify the data.

→ Availability: The network should remain operational all the time. It should be able to provide guaranteed services when an authorized user requires them.

→ Non Repudiation: It is the mechanism to guarantee that sender cannot deny having sent the message & that receiver cannot deny having received the message.

→ Authentication: It is concerned with verifying the identity of the users.

- ISSUES AND CHALLENGES IN SECURITY PROVISIONING -

→ Shared broadcast radio channel: The radio channel used for communication in ad hoc wireless networks is broadcast in nature & shared by all nodes in the network. So, data transmitted by a node is received by all the nodes within its transmission range.

→ Insecure Operational Environment: The environment where ad hoc wireless networks are used may not always be secure. Ex: Networks in battlefields. Hence, they would be highly vulnerable to security attacks.

→ Lack of Central Authority: Adhoc wireless networks do not have any central points to monitor the traffic on the network.

→ Lack of Association: Since these networks are dynamic in nature, a node can join or leave the network at any point of time. Hence, an intruder may join the network & carry out his/her attacks.

→ Limited Resource Availability: Resources such as bandwidth, battery power & computational power are scarce. Hence, it is difficult to implement complex Cryptography based security mechanisms.

→ Physical Vulnerability: Nodes in these networks are compact & hand held in nature. They could get damaged easily & vulnerable to theft.

* Network Security Attacks.

• Network Layer Attacks—

→ Wormhole Attack: Attacker receives packets at one location in the n/w & tunnels them to another location in the n/w.

→ Blackhole Attack: A malicious node that can divert packets by falsely advertising better paths to destination. The intention of malicious node is to hijack path & intercept data packets being sent to destination node.

→ Byzantine Attack: Infected node may create routing loops, route packets to non optimal paths & selectively drop packets.

→ Information Disclosure: Malicious node may leak confidential information to unauthorized nodes in the network.

→ Resource Consumption Attack: Malicious node consumes/wastes away resources of other nodes present in the network.

→ Routing Attacks:

* Routing Table Overflow - A malicious node advertises routes to non existent nodes. Its object is to cause overflow of routing tables.

* Routing Table Poisoning - A malicious node sends fictitious routing updates.

* Packet Replication - A malicisous node replicates stale packets. This consumes additional bandwidth & battery power resources.

• Transport Layer Attacks—

→ Session Hijacking: Malicious node takes control over a session between two nodes.

• Application Layer Attacks -

→ Repudiation:- Repudiation refers to denial or attempted denial by a node involved in communication.

- Other Attacks –

→ Multi-Layer Attacks: These attacks can occur in any layer of the network protocol stack.

* Denial of Service (DoS) Attack: Malicious node prevents authorized users from accessing the service.

Types of DoS Attacks:

→ Jamming: Transmission of signals on frequency of senders & receivers to hinder the communication.

→ SYN flooding: Malicious node sends large number of SYN packets to victim node.

→ Distributed DoS: Several nodes perform attack to prevent authorized users from accessing a services.

* Impersonation: Malicious node pretends to be another node.

* Device Tampering: Mobile devices getting damaged or stolen easily.

Attacks are mainly of 2 types –

1) PASSIVE ATTACKS: In this, system is monitored for vulnerabilities. Hence, purpose of these attacks is just to gain information. No data is changed on the target. Ex: Snooping. Difficult to detect.

2) ACTIVE ATTACKS: In this, network is exploited by a hacker who attempts to change data on a target device. Easily detectable. Ex: Network Layer Attacks, Transport Layer Attacks, Application Layer Attacks, Other Attacks (Done Above).

* Key Management in Ad Hoc Wireless Networks -

- Password-based Group Systems
→ A long string is given as password for users for one session.
→ A strong key is derived from weak passwords given by participants.
→ This can be used for two-party session or a whole group session.

- Threshold Cryptography
→ PKI (Public Key Infrastructure) enables easy distribution of keys. Each node has public/private key pair & Certifying Authority can bind keys to particular node.

- Self organized Public Key Management for Mobile Adhoc Networks
→ Users issue certificate to each other based on personal acquaintance
→ A certificate is binding between node & its public key. These are issued only for specified period of time & contain their time of expiry along with them.

* Secure Routing in Ad Hoc Wireless Networks -

- Requirements of Secure Routing protocol for adhoc wireless networks:
→ Detection of Malicious Nodes → Confidentiality of NW Topology
→ Guarantee of Correct Route → Stability against Attacks

- Secure Routing Protocols:
→ SAR (Security Aware Adhoc Routing) Protocol - It uses security as one of the key metrics in path finding. SAR defines level of trust as measure for routing & establishment.
→ (Secure Efficient Ad Hoc Distance Vector) (SEAD) Routing Protocol: It uses one way hash function & is based on destination-sequenced distance vector (DSDV) routing protocol. It is designed to overcome DoS attacks.

→ Authenticated Routing for Adhoc Networks (ARAN) Routing Protocol:
It is based on cryptographic certificates which defeats identified attacks in network layer.

Unit - III : Ch - 1

WIRELESS SENSOR NETWORKS

* INTRODUCTION :

- Wireless Sensor Network (WSN) is a wireless network consisting of highly distributed wireless devices using sensors to monitor physical & environmental conditions such as temperature, sound, vibration or pressure.
A sensor is a transducer which converts physical phenomenon such as heat, light, sound into electric signals.

- Components of WSN → Each of the node in sensor network consists of three subsystem:
① The Sensor Subsystem → It senses the environment.
② The processing subsystem → It performs computations on sensed data.
③ The communication subsystem → It exchange messages with neighboring nodes.

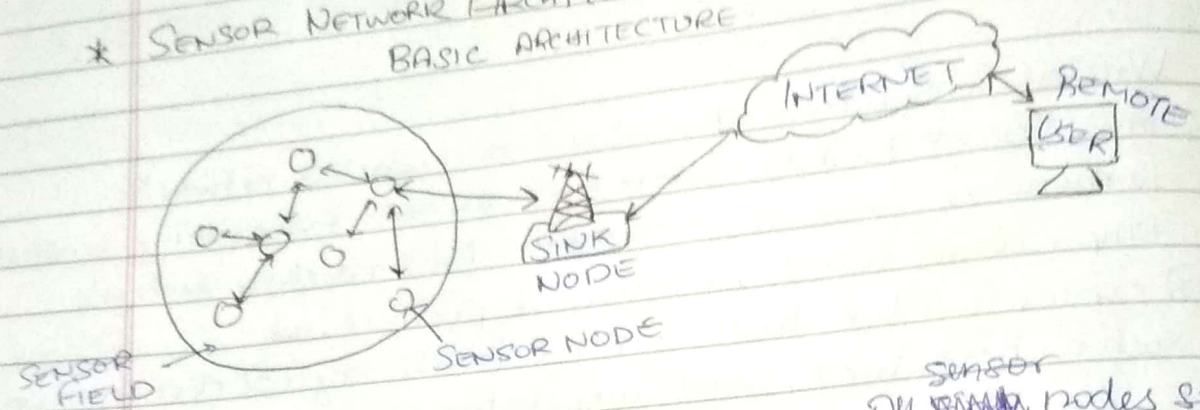
- The network is fault tolerant because many nodes are sensing the same events.

- The nodes cooperate & collaborate on their data which leads to accurate sensing of events in the environments.

- Two most important operations in sensor networks are:
→ Data Dissemination : Propagation of data throughout the network.
&
→ Data Gathering : Collection of observed data from individual sensor nodes.

* SENSOR NETWORK ARCHITECTURE:

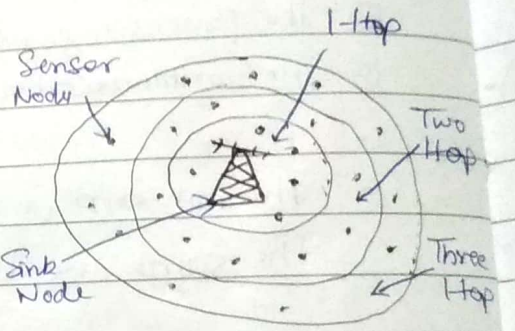
BASIC ARCHITECTURE



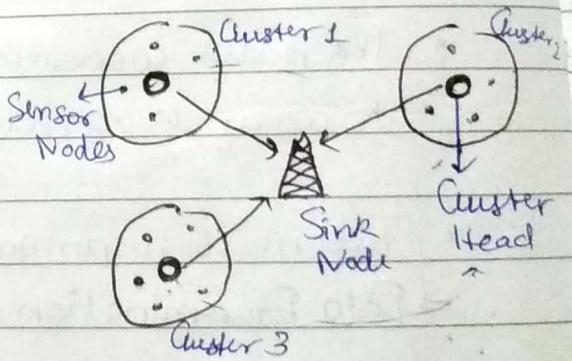
- SINK NODE - They are data collector. All sensor nodes send data to the sink node.
- SENSOR NODE - They are source of information.

Types:

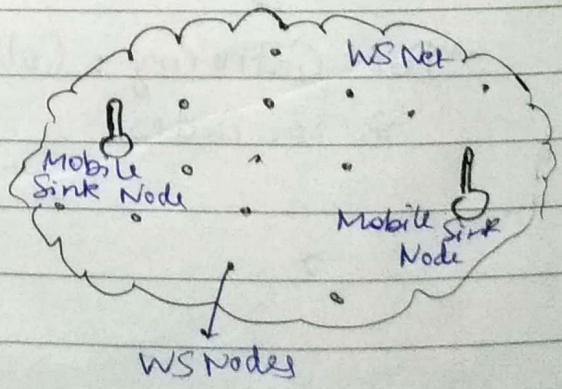
① Layered Architecture - It consists of 1 sink node & multiple sensor nodes that send data to sink node using one hop, two hop etc.



② Cluster Architecture - The node in each cluster sends data to cluster head. These cluster heads sends messages to sink node which is usually a base station.



③ Mobile Sink Node Architecture - The Sink Nodes are mobile & collect data from sensor nodes while travelling in sensing area.



* DATA DISSEMINATION-

It is a process by which data & queries are routed in sensor network. 'Source' is the node that generates the data & 'event' is the information to be reported. A node that is interested in data is called 'sink'. 'Interest' describes for an event that a node is interested in. (A node interested in an event sends 'interest' message)
'Event' is transferred from 'Source' to 'Sink' after 'Source' receives an 'Interest' message from 'Sink'.
Data dissemination is a two step process:

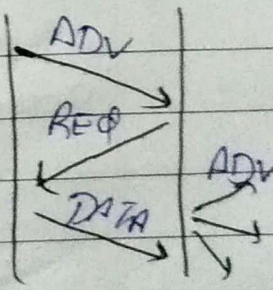
Step 1) Interest of nodes is broadcasted in the network.
Step 2) Nodes after receiving requests sends data having requested data.

Some of data dissemination methods are:

① FLOODING - Each sensor node that receives a packet, broadcasts it to its neighbors if maximum hop count of packet is not reached & node itself is not the destination of packet.

② GOSSIPING - It is modified version of flooding where nodes do not broadcast a packet, but sends to a randomly selected neighbor. It does not guarantee that all nodes of network will receive message.

③ SENSOR PROTOCOL FOR INFORMATION VIA NEGOTIATION (SPIN) - It is enhancement of flooding. The nodes advertise their data & hence, sends their data after receiving a reply from interested nodes. It uses 3 types of messages → ADV, REQ & DATA. Thus, it uses 3 way negotiation before sending the data.



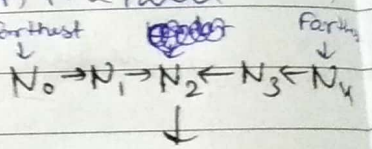
* DATA GATHERING-

The aim of data gathering is to transmit data that has been collected by sensor nodes to the base station. The main purpose of data gathering approaches is to minimize both the energy consumption & delay.

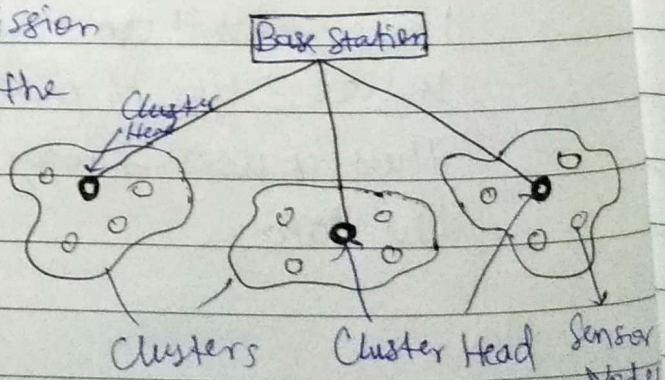
Various data gathering protocols/approaches are as followed:

① DIRECT TRANSMISSION - All sensor nodes transmit their data to the Base Station. This is extremely expensive in terms of energy consumed as BS may be very far away from some nodes.

② POWER EFFICIENT GATHERING FOR SENSOR INFORMATION SYSTEMS (PEGASIS). It assumes that all sensor nodes know the topology of whole network. It forms an open chain starting from the node which is farthest from BS. The chain is constructed before data transmission. Nodes aggregate the data & only one message is forwarded to the next node. The node selected as leader then transmits all data to BS in a single hop. (Leadership is transferred in sequential order) So that nodes know the direction to pass message



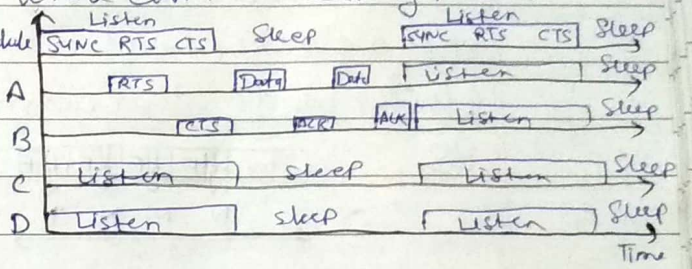
③ LOW ENERGY ADAPTIVE CLUSTERING METHOD (LEACH) - In this, clusters of sensor nodes are formed & cluster heads are used as routers to the sink. It saves energy as transmission is done by cluster heads only & not all the sensor nodes.



* MAC PROTOCOLS FOR SENSOR NETWORKS -

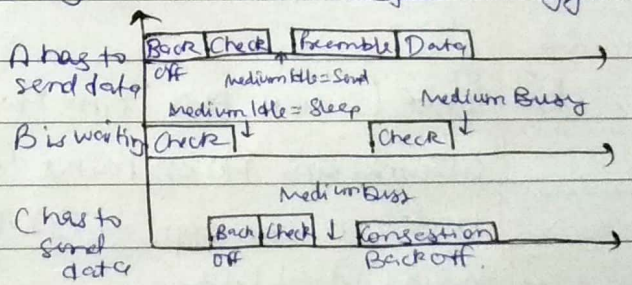
. Contention Based - Medium access is distributed. There is no central coordination for the nodes to use medium. Types:

a) Sensor MAC (S-MAC): It operates by placing a node in a state that listens to the medium. if node hears nothing, it sends a SYNC packet with a schedule, defining listens & sleep periods. All nodes hearing this packet adopt the schedule. During the listen period a node with a packet to send will send RTS frame & receiver will answer with CTS frame. All nodes not involved in this conversation will enter sleep state while communicating nodes send data packets & ACKs.



b) Berkley MAC for Low Power Sensor Networks (B-MAC) - It employs adaptive preamble to reduce idle listening which uses a lot of energy.

→ When a node has a packet to send, it waits during back off time before checking the channel. If channel is clear, the node transmits, otherwise it begins second back-off called 'congestion-back off'. Each node checks channel using LPL (Low power listening). If channel is idle & node has no data to transmit, the node returns to sleep.

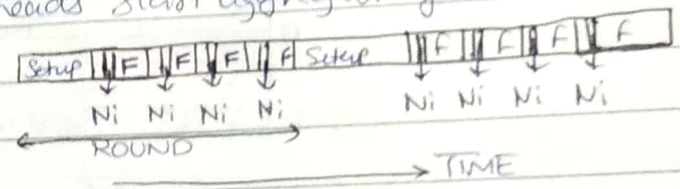


The channel is checked equal to preamble frame size. The receiver detects preamble packet & data is sent by sender.

a] Predictive Wake Up MAC (PW-MAC) - It uses pseudo random schedules. Thus, all node do not wake up & transmit at same time. Hence, avoids collisions. A node that just woke up sends a beacon so that other nodes know it is up. Hence, sender can send data packet & request information from receiver.

- Schedule Based - Medium access is granted by defining an order for nodes to transmit, receive or be inactive. Types:

a] Low Energy Adaptive Clustering Hierarchy (LEACH): LEACH assumes all nodes are synchronized & can control their transmission power & can reach one base station if needed. Nodes organize in clusters, elect a cluster head (CH) & start sending information. Cluster heads start aggregating their cluster data & send it to BS.



LEACH operation rounds. F frames are divided into time slots. 'Ni' are slots assigned to node 'i'.

b] Power Efficient and Delay Aware Medium Access Protocols (PEDAMACS) - It assumes one Access Point (also called sink) with ability to reach all sensor nodes in one hop. PEDAMACS has four phases:

→ Topology Learning → Access point broadcast a packet to synchronize nodes. Hence, each node identifies its local neighbors.

→ Topology Collection → Each node send topology information to the Access Point.

→ Scheduling Phase → AP broadcasts schedule so that every node knows time slots allowed for it to transmit & receive. Rest of the time, node sleeps.

During/
- Adjustment → After scheduling phase, AP requests & nodes send adjustment topology packets indicating changes in the neighbors.

* LOCATION DISCOVERY -

- During aggregation of sensed data, the location information of sensors must be considered.
- Each node attaches its location information with the data in the message it sends.
- Location discovery consist of two components: one is reference points, whose coordinates are known, other is spatial relationship between sensors & reference point.

The problem of location discovery in WSN is overcome by following-

- BEACON BASED SOLUTIONS - (Indoor Localization)

→ Fixed beacon nodes are placed in the field & they know their own locations.
→ The randomly distributed sensor nodes receive beacon signals from beacon nodes & measure signal properties.
→ The nodes estimate distances by using properties found in the database.
→ The database is only carried by BS.

- BEACON LESS SOLUTIONS - (Sensor Network Localization)

→ In situations where no fixed infrastructure is available, the neighboring sensor nodes act as beacon nodes.
→ Through GPS, beacon nodes have their location information & send periodic beacon signals to other nodes.
→ The time difference between beacon arrivals from different nodes can be used to estimate location.

* QUALITY OF SENSOR NETWORK -

→ Purpose of sensor networks is to monitor & report events taking place in a particular area.

→ Hence, main parameters for WSN are as followed:

- Power - It considers most critical limitation. High compression & local data processing is done before dissemination to achieve better QoS.
- Bandwidth - Data compression is used to overcome lack of bandwidth.
- Lifetime - WSN life is limited as nodes operate on unchargable power source like battery & they also undergo node damage. Using solar or wind power to charge battery can be helpful in this case.
- Memory Size - Limited cache memory size affects QoS in WSN.
- Coverage - It defines how well network can observe or cover an event.
  → Worst-case coverage: defines area where coverage is poorest.
  → Best-case coverage: defines area where coverage is best.
- Exposure - It is the expected ability of observing a target in the sensor field.

* EVOLVING STANDARDS -

→ IEEE 802.15.4 Low Rate Wireless Personal Area Network (LR-WPAN) standard focuses on low cost communication with multi year battery life & very low complexity.

→ Low power consumption is an important feature targetted by this standard.

→ It requires less transmission rate, power efficient modulation techniques & strict power management techniques such as sleep modes.

* OTHER ISSUES -

• Design Issues

→ Fault-tolerant Communication: Sensor nodes are deployed in harsh environments, hence, sensor nodes become faulty & unreliable.

→ Scalability: A system whose performance improves after adding a hardware; proportional to capacity added, is called scalable system.

→ Coverage Problems: It defines how well a network can observe or cover an event.

• Topology Issues

→ Geographic Routing: It is routing principle that relies on geographic position information i.e, source sends message to geographic location of destination instead of using network address.

→ Sensor Holes: A routing hole is region in sensor network where either nodes are not available or available nodes can't participate in routing.

• Other Issues

→ Deployment

→ Hardware & Operating System for WSN

→ Synchronization

→ Localization

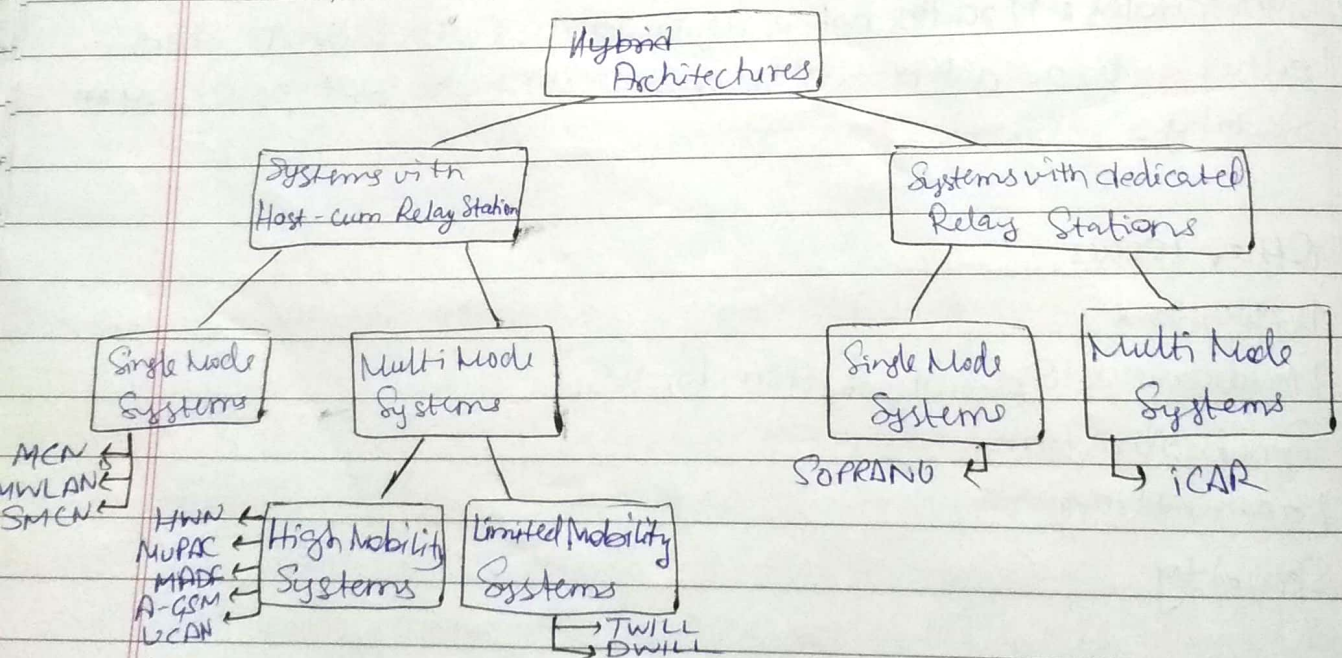
→ Security

Unit-3: Ch-2

* HYBRID WIRELESS NETWORKS (INTRODUCTION)

- These networks are made by adding base stations to adhoc network.
- It can act as Base Station & Ad-Hoc Network according to the environment conditions.
- It has advantages of both Ad-Hoc & Base Station.
- Mobile nodes communicate with each other using Ad-Hoc mode when they are in range & use Base station to communicate when they are out of range.
- They are more efficient & reliable. Highly scalable & better performance.

* NEXT GENERATION HYBRID WIRELESS ARCHITECTURE-



- HOST CUM RELAY STATION- In this, dedicated relay station do not originate data traffic on their own & assist in forwarding on behalf of the sender.

- SINGLE MODE SYSTEMS: Mobile Hosts operate only in Multi Hop mode.
  - * MCN- Multi Hop Cellular Network
  - * MWLAN- Multihop WLAN
  - * SMCN- Single Interface Multihop Cellular Network

- MULTI MODE SYSTEMS: The mobile hosts can act either in single hop mode or multihop mode depending on the architecture.
  - High Mobility Systems - (Systems with high mobility) Hybrid Wireless Network (HWN), Multi Power Architecture for Cellular Networks (MuPAC), Unified Cellular & Ad Hoc Network (UCAN), Mobile Assisted Data forwarding (MADF), Ad-hoc GSM (AGSM),
  - Limited Mobility Systems (Systems with Limited mobility) - Throughput Enhanced Wireless in Local Loop (TWiLL) Directional throughput-enhanced wireless in Local Loop (DWiLL)

- DEDICATED RELAY STATIONS - Dedicated relay stations are used for relaying data traffic.
- SINGLE MODE SYSTEMS: Self Organizing Packet Radio Ad-Hoc Networks with Overlay (SOPRANO)
- MULTI-MODE SYSTEMS: Integrated Cellular & Ad Hoc Relaying System (ICAR).

(velchuriblog.files.wordpress.com/2016/12/wsn_c-siva-ram-murthyb-s-manoj.pdf)

^ To study each architecture in detail.

* ROUTING IN HYBRID WIRELESS

• Base-Assisted Ad Hoc Routing- (BAAR)
- This protocol was proposed for MCN architecture.
- It efficiently makes use of BS for routing.
When a BS receives RouteRequest from a node, it uses BAAR protocol to compute the route as follows:

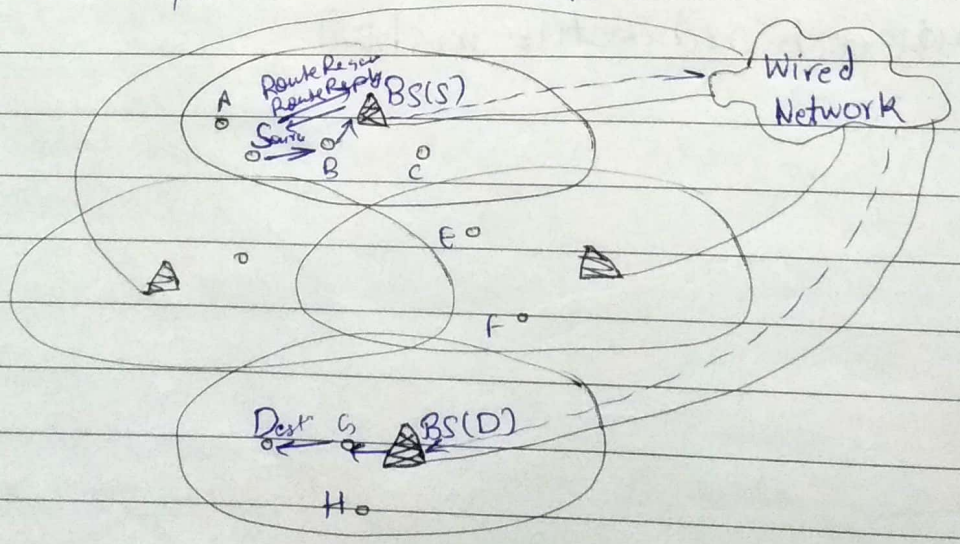
Operation of BAAR Protocol

Here, BS(x) denotes the BS to which node x is registered.

1) If BS(S) = BS(D) [Source & Destination in common cell]
→ Run shortest path algorithm over all wireless links in common cell.

2) Else If BS(S) & BS(D) are BSs in adjacent cells,
→ Get state of links in adjacent cells to which node D belongs.
→ Run shortest path algorithm over all wireless links in two adjacent cells including the link between BS(S) & BS(D).
→ Return path obtained.

3) Else [If nodes are not in common or adjacent cells]
→ Run shortest path algorithm over all links in node S's cell & obtain shortest path (p1) from S to BS(S).
→ Similarly obtain shortest path (p2) from D to BS(D).
→ Return p1 (BS(S), BS(D)) p2.



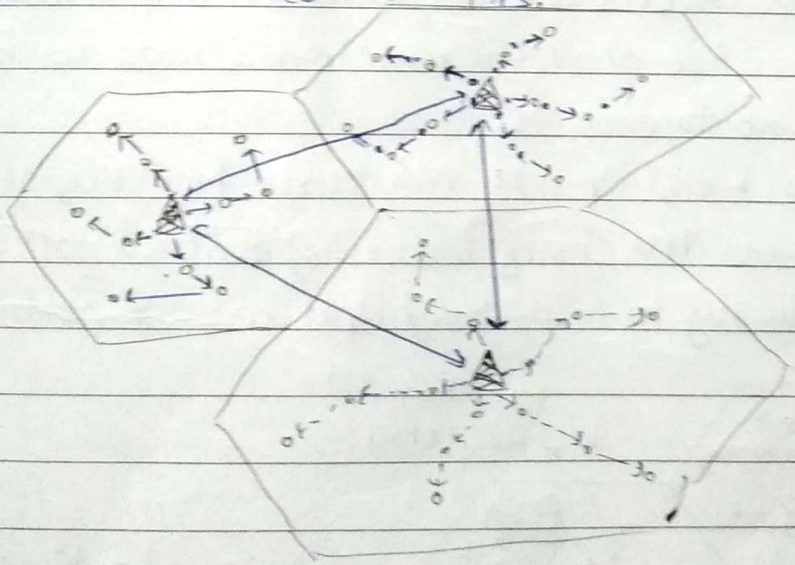
[All BS are connected to wired Network]

Source Node & Destination Node Belong To Non Neighboring Cells. (Similarly for Other Two Cases)

- Base Driven Multi Hop Bridging Routing Protocol - (BMBP)
  - This protocol was proposed for Multi Hop Wireless LANs (MWLANs).
  - BMBP resides partly in Mobile Stations (MS) & partly in Access Points (AP) to enable multi hop routing.
  - AP computes a routing table called bridging table for a particular MS which includes next-hop node & hop count.

Messages used in BMBP.

1) Beacon - It is periodically generated by AP to advertise its presence to the MS in its cell. The Beacon packets are forwarded by MS which receive them. They also carry hop count information which is incremented by every intermediate node that forwards it.
2) Hello - These are generated by MSs towards their associated APs. Each MS appends its own information as it forwards Hello.
3) Bridge - It is originated by AP periodically. It contains routing topology of the network.
4) Care-of - It is for information interchange over wired networks that interconnects the APs.



o - MS

△ - AP

⟷ - Care of Message

⇢ - Beacon Message

⟶ - Bridge Message

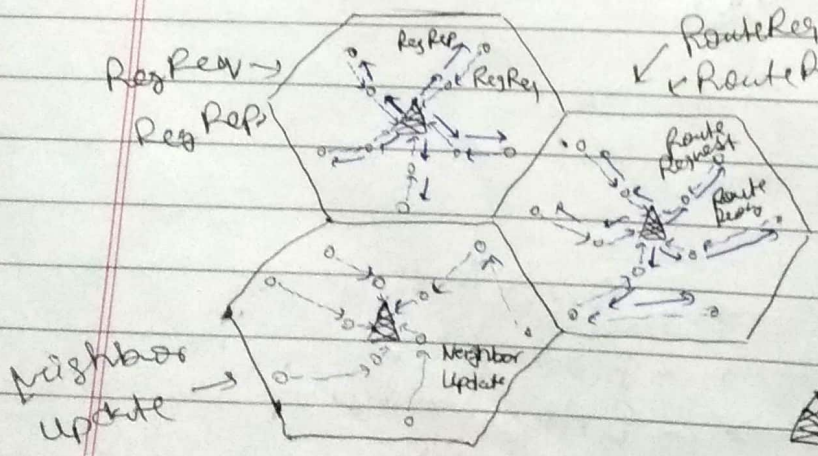
⟶ - Hello Message.

SMCN Routing Protocol /

- Single Interface Multi Hop Cellular Network Routing Protocol - (SMRP)
- This protocol was proposed for Single Interface Multi-Hop Cellular Network (SMCN).
- It provides mechanisms for routing both control & data packets through multiple hops.
- SMRP routes control packets efficiently & also finds nearest BS for a MS & register the MS with that BS over multiple hops.

Messages used in SMRP-

- Registration Request (RegReq): MS sends RegReq to the nearest BS so as to request to be registered to that BS.
- Registration ACKnowledgement (RegAck): BS generates RegAck in reply to RegReq. MS registration is completed when it receives RegAck.
- RouteRequest: When a packet arrives at MS, it will send RouteRequest to its BS requesting for a path to the destination.
- RouteReply: BS finds shortest path to destination & sends it to the MS through RouteReply packet.
- Beacon: Each node (both MS & BS) generate beacon messages periodically. It contains information about the route from a node to different BS & also the hop count to each BS.
- Neighbor Update (NeighUpdt): MS sends NeighUpdt message to BS informing it of the changes in neighborhood topology. Each MS checks periodically to see if NeighUpdt message needs to be sent to BS



SMCN Routing Protocol.

- Base Station
- Mobile Station

Date
Page

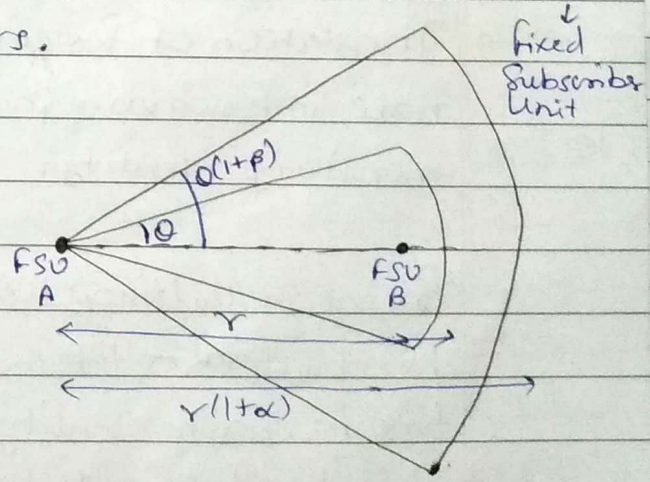
DWiLL Routing Protocol (DRP)-

- This protocol was introduced for DWiLL Architecture.
- It uses multihop relaying with directional antennas.

Operation of DRP

- Each node reports the set of nodes from which it receives Beacon.
- BS builds up two topology matrices: Multihop Connectivity Graph (MCG) & Single Hop Connectivity Graph (SCG). It also builds up two interference matrices: r-interference matrix for multi hop channel & R-interference matrix for single-hop channel interference.
- The r-interference matrix & the R-interference matrix contain the information regarding interference on channels used in MCG & SCG respectively.
- The Beacon packets are received with high power which causes interference within directional sector of radius $r(1+\alpha)$ & angle $\theta(1+\beta)$. where 'r' is multihop channels' transmission range & 'θ' is azimuth of directional antenna. (azimuth is angular extent from BS to FSU) 'α' & 'β' are interference parameters.

- When a source node needs to set up a call session with another node, it requests the BS by sending a RouteRequest packet. The BS uses DRP to obtain the path to the destination node & replies with RouteReply packet to the sender node.



INTERFERENCE REGIONS IN DIRECTIONAL TRANSMISSION SYSTEM

* PRICING IN MULTI HOP WIRELESS NETWORKS-

- Issues in pricing in Multihop Networks:
  → Reimbursement - Every intermediate node that forwards a packet on behalf of other node is reimbursed for the resources that it has spent. Hence, the extent of reimbursement is a significant factor that determines extent of intermediate nodes to which they can spend power for others.
  → Fairness - It is one of the major concerns of pricing. It is based on the idea that every node pays an equal amount of traffic it has generated.
  → Service Provider Revenue - Service Provider is responsible for providing network access & hence, profit earned by provider is a prerequisite for the network to function.
  → Secure Transfer of Accounting Information - There must be secure means of transmitting the pricing information to a trusted accounting station. (Security over wireless n/w. is a major issue)
  → Translation of Resources Spent into Cost - The power spent by a node in forwarding packets for other nodes has to be converted into monetary identity.

- Pricing in Multihop WAN - In metropolitan areas, providing low-cost, high-bandwidth Internet access with low deployment cost & setup time has become reality with the emergence of Wide area adhoc wireless networks. Hence, all the issues of pricing must be addressed carefully.

- Pricing in adhoc networks - In this, pricing framework should be decentralized due to absence of supporting infrastructure in adhoc n/ws.

- Pricing in Multi Hop Cellular Network (MCN) - The MCN use a Micropayment Scheme for pricing purpose.

Micropayment scheme has four major components -

1) Strategy for users to determine how packets should be routed.
2) Verification module at BSs to check for valid payments.
3) A technique that selects intermediate nodes eligible for payment for their forwarding service.
4) An auditing technique that detects cheating among nodes.

* Power Control Schemes in Hybrid Wireless Networks -

- Power Control Schemes are designed to serve large number of power constrained mobile nodes.
- Based on topology of the n/w formed by mobile nodes, BS estimates minimum power to acheive connectivity.
- Hybrid wireless networks utilize power control to maximize system throughput.

Schemes -

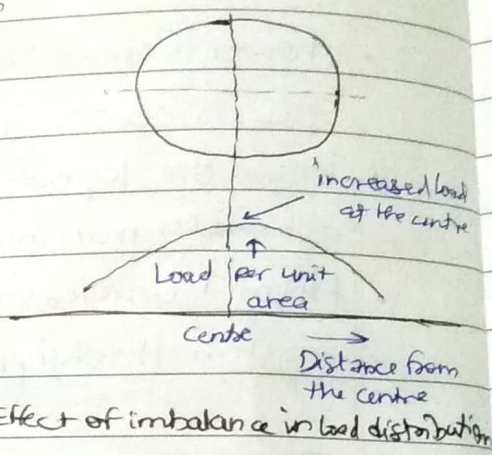
- Power Aware Routing: It uses battery life of the node as routing metric. Hence, Power aware routing minimizes the energy consumed per packet, cost per packet & the cost of node.

- Sleep Scheduling: The sleep scheduling mechanisms are used in Wireless Networks as they can save significant amount of energy by turning off the redundant nodes in the network.

- Energy Harvesting: It is done by attaching the solar panel to the wireless device. These solar panels are made up of photovoltaic cells that convert sunlight to electric current.

* LOAD BALANCING IN HYBRID WIRELESS NETWORKS -

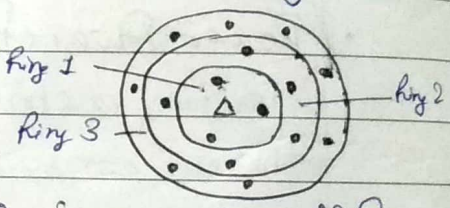
Load balancing refers to the distribution of relay traffic load uniformly throughout the network so that no region in network is overloaded.
Since the relay traffic is highest at centre of network, & decreases with increase in distance from the centre, hence it leads to rapid draining of battery of nodes at centre of n/w. Hence, load balancing is important in hybrid wireless networks.



Effect of imbalance in load distribution

Load balancing schemes:

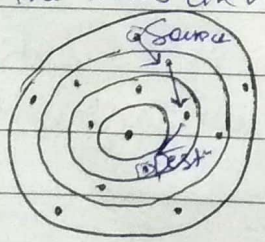
1) Preferred Ring Based Routing Schemes -
In this, the centre of the network is determined at first. Then network is divided in the form of imaginary rings about centre. The choice of number of rings is decided by the base station.



There are 3 schemes for load distribution:

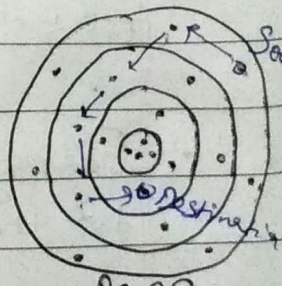
① Preferred Inner Ring Routing Scheme:
In this, a packet must be routed towards the inner ring, if Sourc & Dest^n are in different rings.
& the nodes are in same rings, packet must be transmitted in same ring.

PIRS



So, source is in ring 4 & dest^n is in ring 2. Hence, no transmission must occur in ring 0 or ring 1.

② Preferred Outer Ring Routing Scheme: It is reverse of PIRS. In this, packet remains for maximum time in outer rings of source & destination.
The packet must be routed through outer rings.
If nods in same ring, packet transmission also in same ring.



2) Load Adaptive Routing Scheme:
This scheme consider traffic load at every intermediate node to make load balancing decisions. The measure of load balancing can be regulated from traffic fairness. Traffic fairness is the ratio of load experienced by a node to the average load of entire network. Some of the heuristics for dynamic load balancing & traffic fairness are as followed:

① Preferred Hybrid Routing Scheme (PHRS): This is hybrid of basic schemes such as PIRS, PORS. Thus, a node evaluates path using PORS & PIRS & hence, chooses the least loaded path.

② Base Station Support Reconfiguration (BSR): This routing scheme is applicable only for MCNs where BSs help nodes in path finding during routing. In BSR, the BS reconfigures the path for the nodes which are experiencing low throughputs. The reconfiguration of path tends to redistribute the load from hotter regions (heavily loaded regions) of the network to the cooler regions (lightly loaded regions).

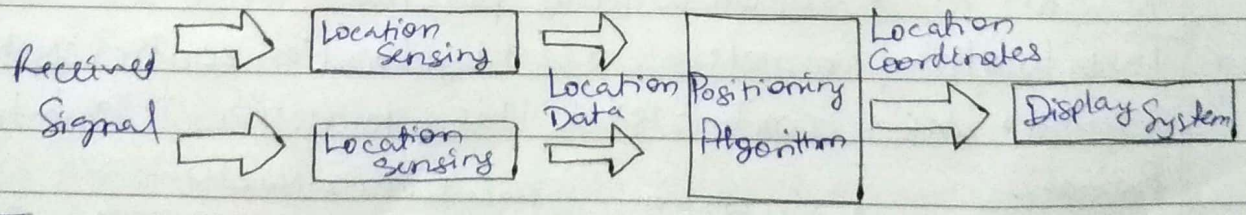
Unit-IV: Ch-1

* Introduction -

- Geolocation, position location & radio location are terms used to describe the ability to determine the location of a MS.
- Location includes the information such as longitudes & latitudes where the MS is located
- Commercial applications include the need for hospitals to locate patients & the equipments, in homes to locate children & pets & in 4G networks, it provides location services.

* What is Wireless Geolocation?

- The term 'location-based service' denotes the services being provided to mobile users based on their geographical location.
- Wireless geolocation systems determine the location of a mobile node with the help of a geolocation infrastructure.
- A wireless geolocation system has 3 major components:
  - A location sensing device that determines relative position of mobile device.
  - The position algorithm that estimates position of mobile device by computing data from location sensing device.
  - The display system which displays computed position of mobile device.



- There are numerous applications such as Mapping Services that provide driving directions; information services that provides news, weather, traffic etc. which are based on Geolocation services.
- Indoor geolocation applications are directed towards locating People & assets within buildings. ex: finding mentally impaired people in hospitals.

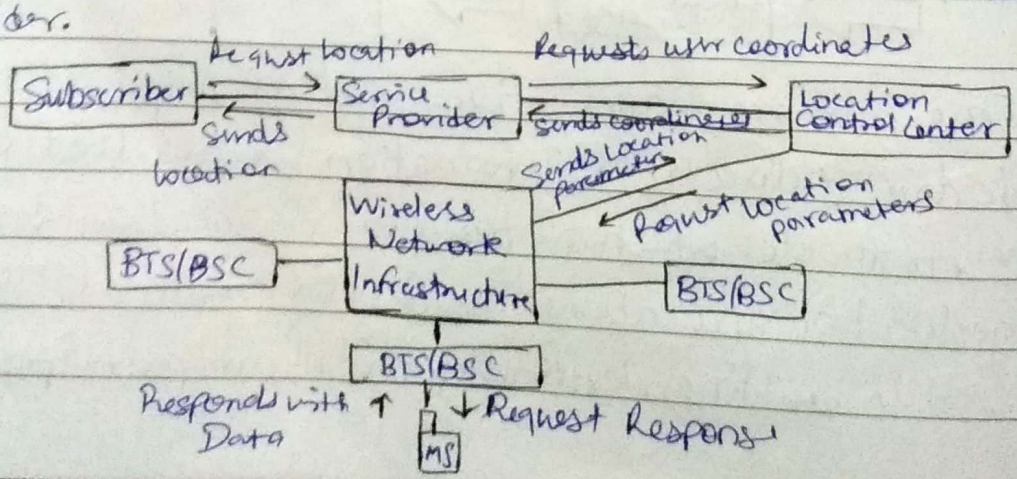
* Wireless Geolocation System Architecture -

The Geolocation System measures the parameters of radio signals that travel from a mobile to receiver or from transmitter to mobile. This is done by positioning system. Types of positioning system -

1) Self Positioning System - MS can locate its own position by measuring its distance from known locations.
2) Remote Positioning Systems - The receivers at known locations in the network compute the location of MS by measuring distance & direction from receivers to this MS. These are also called Network based positioning systems.

Architecture -

- Thus, these two types of positioning system are used for location estimation. This information is shared with the network.
- The subscriber requests location information from Service Provider.
- Service provider sends location information to the Subscriber.
- After receiving request from subscriber, the service provider contact Location control center which gathers information to calculate location of MS.
- Depending on past information about MS, a set of BSs are used to locate MS & obtain location parameters.
- These location parameters are used by location control center to determine MS's coordinates & this information is sent to Service Provider.



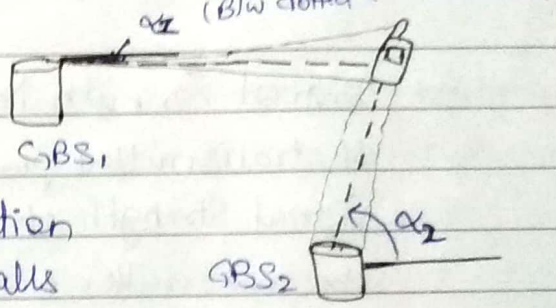
GEO LOCATION SYSTEM ARCHITECTURE

* TECHNOLOGIES FOR WIRELESS GEOLOCATION-

In order to determine coordinates of MS, the distance & direction MS is estimated by Geolocation Base Stations from the received signals. (GBS)
Distances are determined by properties of signals received such as signal strength, signal phase or time of arrival.
Directions of MS can be determined from angle of arrival of received signals.
Techniques used-

i) DIRECTION BASED TECHNIQUES-

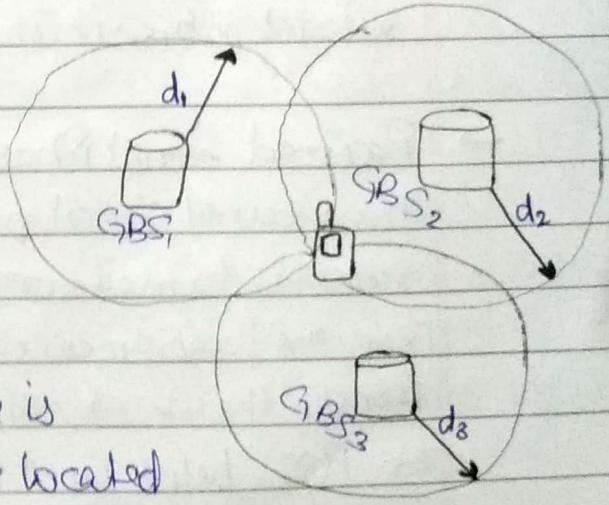
→ The angle of arrival (AOA) geolocation technique uses direction of arrival of received signal.
The receiver measures direction of received signal (i.e the AOA) from target transmitter.



AOA is not suitable for indoor geolocation system as surrounding objects or walls block the signal path.

ii) DISTANCE BASED TECHNIQUES-

The distance between MS & receiver is estimated by using received signal strength & time difference of arrival (TDOA) techniques.
If the distance b/w receiver & mobile is estimated to be 'd', the mobile can be located on a circle of radius 'd' centred on receiver.



→ Arrival Time Method

- A signal travels with speed of 3×10^8 m/s which can be used to determine distance b/w transmitter & receiver. This is the TOA technique.

When GBS detects signal, TOA is determined. If time at which MS transmitted signal is known, the difference b/w TOA & this time gives time taken by signal from MS to reach GBS.

- In GPS, the time difference of arrival (TDOA) technique is used where difference in TOAs are used to locate mobile. Compared to TOA method, main advantage of TDOA is that it doesn't require the transmit time of signal from MS.

→ Signal Strength Method (RSS - Received Signal Strength)

If transmitted power at MS is known, measuring the Received Signal Strength at GBS can provide an estimate of distance b/w the transmitter & receiver.

Since, TOA doesn't distinguish b/w signal stength in LOS path & in reflected paths, it is very unreliable.

→ Received Signal Phase Method

The received signal phase is an important metric. With use of receivers to measure carrier phase, differential GPS (DGPS) can improve location accuracy from 20m to 1m.

Hence, the use of signal phase method along with TOA/TDOA or RSS helps in the fine tuning of the location estimate.

iii) FINGERPRINTING BASED TECHNIQUE-

The multipath structure of channel is unique to every location & can be considered as a fingerprint or signature of the location if same signal is transferred from that location.
This property is used to develop a 'signature database' of various locations.
So a signal received from a transmitter is compared with the entries in database & thus, its location is determined.

* GEOLOCATION STANDARDS FOR E-911 SERVIES-

- E-911 stands for Enhanced 911 Services which are primary driving force for geolocation services. GPS provides sufficient accuracy for E-911 Systems.
- E-911 is a system used in North America to automatically provide the location of callers to 911. It is the universal emergency phone number in the region.
- A new technique called assisted GPS (AGPS) has been proposed which enables the network entity to detect signals with weaker strengths than MS. This allows use of GPS even indoors.
- Technologies used in E-911 Services to determine the location of caller or handset are:
  - → Angle of Arrival (AOA) → direction of arrival of received signal.
  - → Time Difference of Arrival (TDOA) → difference of TOA to determine distance of MS from receiver.
  - → Location signatures or 'fingerprints' to store & recall patterns which mobile phone signals exhibit.
- Location is important concept in working of E-911 System. Hence location is determined by Automatic Location Information (ALI) database which is maintained by 3rd parties for the governments. Thus, ALI database is queried to determine the location of caller.

* PERFORMANCE MEASURES FOR GEOLOCATION SYSTEMS—

- Wireless systems are focused on performance issues such as QoS, reliability, coverage etc. of the networks.

Accuracy
- The most important performance measure of a geolocation system is the accuracy with which location is determined.
- This accuracy depends on environment, receiver, noise & interference.

Location Availability
- The probability that a location request will not be fulfilled is also a measure of QoS for geolocation system. The location request will not be fulfilled if TOA, AOA or other measurements are not available in sufficient number.

Coverage
- In geolocation system, coverage corresponds to availability of sufficient number of TOA, AOA or other measurements (fingerprint) to compute location.

Miscellaneous
- Other measures in geolocation system are delay in triggering location measurement, network transmission delay, database look-up time, end-to-end delay between the time when a location request is made & that information is received.
- Reliability is the mean time between failures & the mean time to repair.

Capacity
- Capacity is another measure that is the number of location requests that can be handled by a geolocation system.

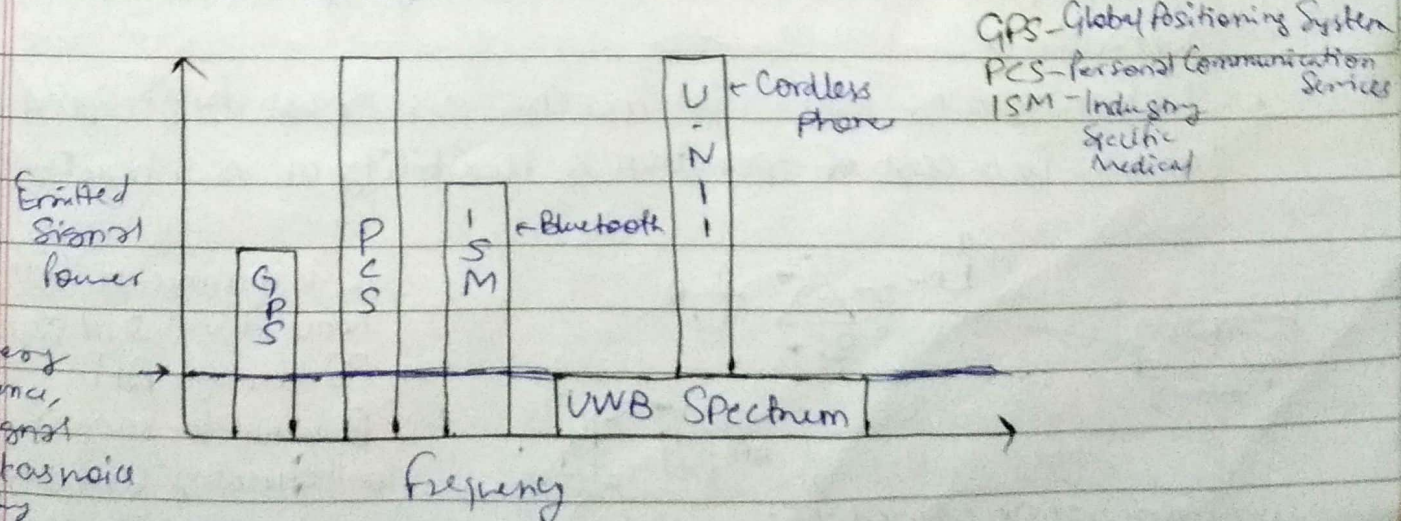
Unit-IV: Ch-2

* Introduction -

- By the end of this decade, internet access will be offered wireless networks.
- To support high data rates on short ranges, technologies such as Ultra Wideband (UWB) transmission scheme & optical wireless networks are being researched.
- Areas of interest include seamless handoff across networks, support for multimedia traffic, all internet services at affordable costs.
- Wireless Fidelity (Wi-Fi) system is the first step in this process which provide high speed WLAN.

* Ultra Wideband Radio Communication -

- UWB is a technology developed to transfer large amounts of data, wirelessly over short distances over very wide spectrum of frequencies in short period of time.
- UWB technology has the capacity to handle very high bandwidth which are required to transport multiple audio & video streams.
- It will be ideal for transmitting data between devices within short range at high speeds while consuming little power.
- It doesn't cause interference to other radios such as cellphones, TV broadcast sets etc.



UWB Spectrum Comparision

Advantages-

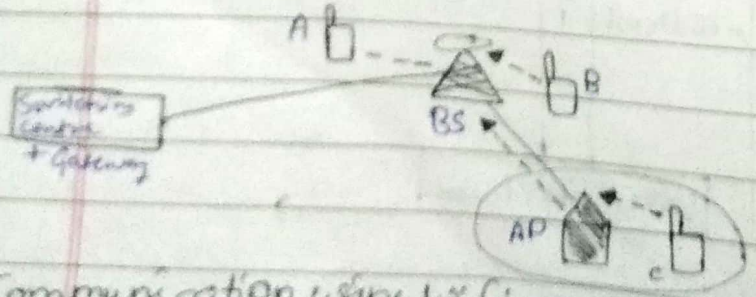
- Extremely Difficult to Intercept: Wideband pulsed radar spreads the signal & allows more users to access scarce frequency spectrum.
- Multipath Immunity: It doesn't interfere with other services.
- Precision: Real time position down to centimeter of resolution in Systems.
- Low Cost: Requires minimal components resulting in small size & weight.
- Low Power: Power consumption is in Microwatts which is very low.

Applications-

- Communications: High speed WLANs, Mobile adhoc wireless Networks.
- Sensor Networks: Ground penetrating radar, short range motion sensing.
- Tracking/Positioning: Precise geolocation System & high resolution imaging Tracking (indoor/outdoor) down to less than a centimeter.

* WIRELESS FIDELITY SYSTEMS-

- Wireless fidelity (Wi-Fi) is the standard for high speed wirless LAN.
- Wifi can be used to connect computers to each other, to the Internet & to the wired networks.
- Wifi provides high speed multimedia content delivery.
- Integration of Wifi hotspots (WLAN Access Points) provided an additional advantage for mobile nodes. Such an integrated system provides secure, reliable & high speed wireless connectivity.
- Advantages of Wifi systems are ease of use, high speed internet access, low cost of operation & flexibility of reconfiguration.



Communication using Wifi or BS

C is in range of Wifi AP & hence it will send signal to BS through AP.

B is not in range of Wifi & will directly send signal to BS to establish communication with B.

Issues in Wi-fi Systems:

- Security: Since Wifi uses radio signals for connectivity, it is prone to various attacks that tend to challege the security of Wifi services. Hence security is the main issue in Wifi Systems. The major elements that cause vulnerability to Wifi systems are -
  - → Eavesdropping - Also known as sniffing or snooping. In this, the attacker tends to intercept the communication & steal the information. Unsecured wireless networks are prone to this type of attack.
  - → The Rogue Client - The authenticated client has intentions of acting against the organisation is a problem faced by wireless networks.
  - → Session Hijack Attack - In this, the attacker waits until authentication of a node with an AP. On completion of authentication, the attacker sends a forged message which disassociates the original node. Now, attacker uses originally authenticated node's address to utilize its service
  - → Man-in-the-middle Attack - In this attack, the attacker represents itself as an AP & the connection b/w two parties is established through this attacker. Thus, attacker is able to read messages, change data etc.

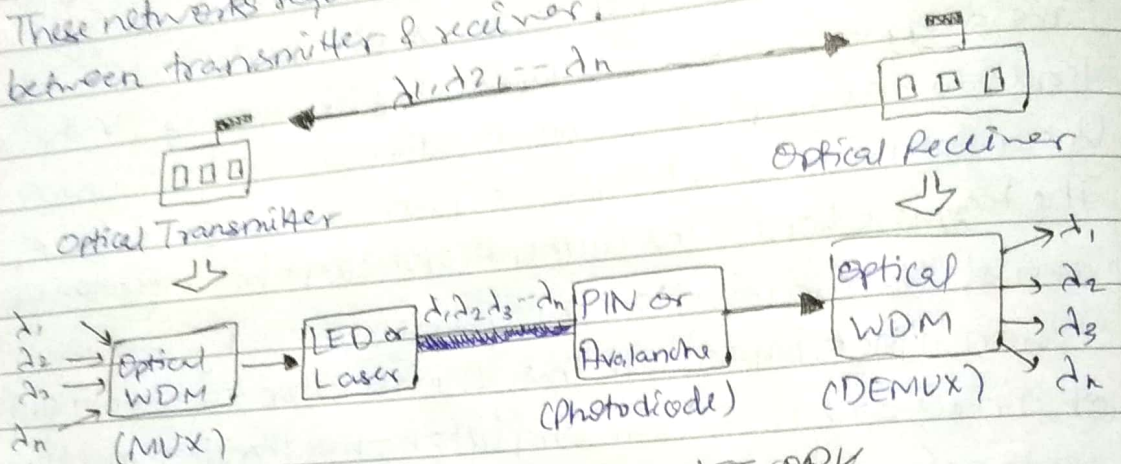
- Authentication - Authenticating the nodes being connected is another issue involved with Wifi Systems. Various authentication measures such as Certificate-based authentication, tokens, one-time passwords (OTPs), Kerberos etc. are applied by extendible authentication protocol (EAP).

- Quality of Service (QoS) - Provision of QoS is important in traffic such as voice & video.

- Billing Schemes - flat rate schemes (for unlimited bandwidth, fixed time) & volume based schemes (on basis of amount of data used) are used to charge the customer for his Wi-fi usage.

OPTICAL WIRELESS NETWORKS-

- Communication in optical wireless networks is established using Infrared Rays & Light Rays.
- These networks require Line of Sight communication between transmitter & receiver.



OPTICAL WIRELESS NETWORK

WDM → Wavelength Division Multiplexing

- Optical Transmitter consists of Optical Multiplexer, LED/Laser device.
- Optical Receiver consist of Optical Demultiplexer & detector circuit using PIN/Avalance Diode. (PIN → p-type intrinsic n-type)

→ Optical MUX multiplexes various wavelength channels for simultaneous transmission & Optical DEMUX does the opposite at receiving end.

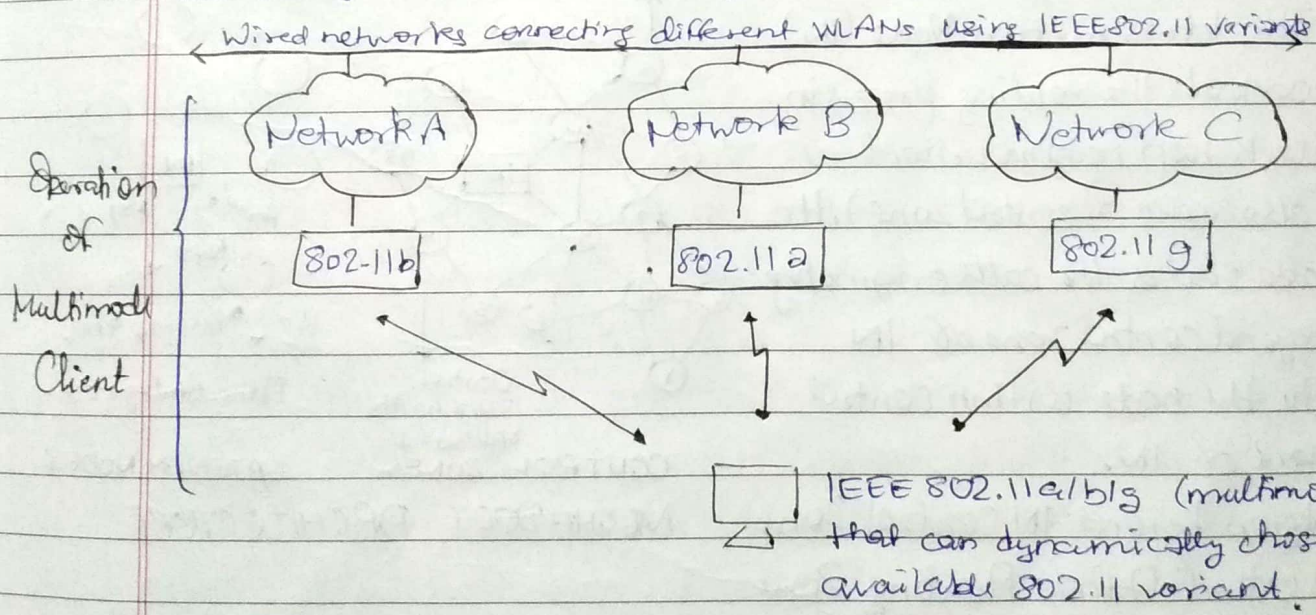
→ There are different topologies supported in optical wireless system: point to point, point to multi point & ring bus.

ADVANTAGES- Cost effective at rates near 100 Mbps, Higher capacity, Highly secure as optical wave do not penetrate the walls, No multipath fading, Immune to interference

DISADVANTAGES- High Power Requirement, Limited Range, LOS Link break can lead to tremendous loss of data. Costly for low rates, environment conditions can cause link failures such as smoke, rain, birds etc.

* THE MULTIMODE 802.11 - IEEE 802.11a/b/g :

- The Multimode 802.11 can operate in all the three major variants of IEEE 802.11 standards which are 802.11a, 802.11b & 802.11g.
- It is the WLAN client interface implementation that can work with APs operating according to any of the three IEEE 802.11 standards.
- At any given time, IEEE 802.11 a/b/g interface works with only one AP.
- The multimode WLAN clients that are 802.11a/b/g compatible can connect to any 802.11 AP transparently, leading to enhanced roaming services across different networks.
- An 802.11a/b/g client that detects carriers from different APs using 802.11a, 802.11b, & 802.11g is shown as follows:

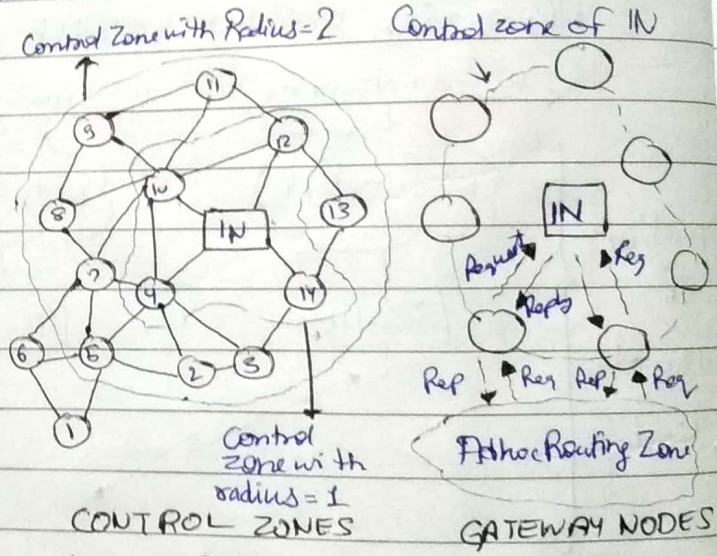


- The 802.11a/b/g client searches for carrier in all the bands & selects the most appropriate one.
- Hence, new generation of WLANs are capable of operating in all these different modes.

* THE MEGHADOOT ARCHITECTURE -

- It is a packet based wireless network architecture for low cost rural community networks.
- This architecture is an alternative to costly Wireless Local Loop (WLL) which provided communication services in rural regions.
- Meghadoot is a Sanskrit word, meaning 'Cloud Messenger'.
- Major goals of Meghadoot Project are:
  - → Develop a fully distributed packet based hybrid wireless network that can carry voice & data traffic.
  - → Provide low cost communication in rural areas.
  - → Provide low cost communication in urban areas.
- Meghadoot uses an 'infrastructure based adhoc routing protocol (IBAR).
- The Infrastructure Node (IN) controls the routing process in its K-hop neighbourhood (also known as control zone). It also routes the calls originating beyond control zone of IN to the node within control zone of IN.
- Region beyond IN control zone is called Adhoc Routing Zone
- Meghadoot uses Gateway Nodes (GNs) for interfacing the nodes in the adhoc routing zone to the IN so that such nodes find routes efficiently to the nodes inside the Control Zone of IN.
- Nodes in adhoc routing zone broadcast RReq packet which is routed by GN to IN. When RReq reaches IN, it replies with RRep packet if the destn node is in control zone to GN. GN then sends it to original sender.

(Source) (Destination) (not broadcasted)



MEGHADOOT ARCHITECTURE

* VEHICULAR SENSOR NETWORKS-

- Driving is the most dangerous task people do everyday. People are involved in accidents almost everyday around the world.
- Since, driving is a data driven task, the vehicles are equipped with short range & medium range wireless communication & hence, vehicles act as nodes & form a network.
- These are called Vehicular Sensor Networks in which the cars/vehicles have two kinds of communication:
  - V2V (Vehicle to Vehicle)
  - V2R (Vehicle to Roadside Units)

  Hence, communicating vehicles & roadside infrastructure collectively form a sensor network.
- This network is based on VANET (Vehicular Adhoc Networks) which is a particular kind of a MANET (Mobile Adhoc Network).
- Components in Vehicular Sensor Networks:
  - Mobile Sensor Nodes: These are embedded on vehicles.
  - Stationary Sensor Nodes: These are deployed at a predetermined distance beside the road.
  - Base Station: These are traffic control check post, fire station etc.
- Applications of Vehicular Sensor Networks:
  - Collision avoidance at intersections (ex: pedestrians, cyclists etc.)
  - Traffic congestion information.
  - Ambulance approach warnings & routing
  - Parking Lot Information
  - Marketing & Advertising
  - Drunk Driver Detection
  - Car to car messaging or voice
  - Local Area Information.