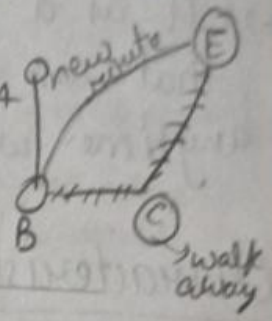
Wireless Adhoc and Sensor Networks

→ wireless n/w
→ consist of a set of mobile nodes connected wirelesely in a self-configured, self-healing n/w without having a fixed infrastructure
→ utilize multi-hop radio relaying - no router no tower
→ Dynamic Topology
→ may operate a standalone or they can be a part of large internet.
→ peer-to-peer, self-forming n/w.
→ Uses → road safety, home, health,
→ disaster rescue opera^



Cellular N/w	Adhoc wireless N/w
→ Infrastructure based.	→ Infrastructure-less
→ Single-hop	→ multiple-hop.
→ Guranteed Bandwidth	→ Shared-radio channel (No-P Goarantees)
→ Circuit-Switched (perform)	→ Packet Switched
→ Centralized routing	→ Distributed routing.
→ High cost / time for deployment	→ Quick and cheap deployment
→ High maintainance cost	Low Main. cost.

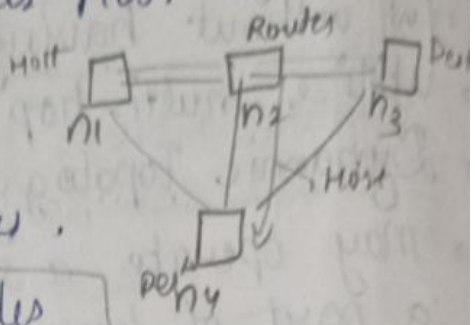
Types wireless N/w
→ Homogeneous → similar char. device
→ Heterogeneous → diff. " "

MANET → wireless n/w
→ No fixed infrastructure (nodes are mobile in nature)

→ Dynamic Topologies

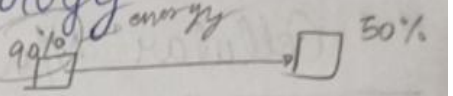
→ NODE in MANET can act as HOST or ROUTER

→ MANET is a autonomous coll" of mobile users that communicate over wireless links.



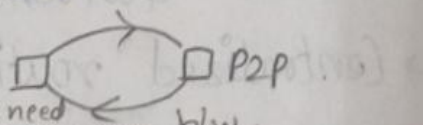
→ It is a collec" of mobile nodes that can be dynamically set up anywhere, anytime without the use of pre-existing infrastructure

Characteristics → Dynamic Topology
→ form bidirec" or multidirec - link

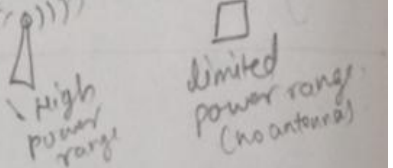


→ Energy constrained nodes.
→ Limited security } because no infrastructure not centralized.
→ Autonomous → node ⇄ host / router.
→ Distributed.

Properties → Fast n/w Establishment
→ Peer-to-peer connectivity



→ no need of any server b/w.
→ Independent computation
→ No. req. of access point. (because not centralized)
→ Less wireless connectivity Range.
(It can only connect nearby nodes)



→ MANET nodes can be mobile phones, tablets, laptops, smart sensors etc.
→ Uses a variety of protocols → Bluetooth, TCP/IP, GSM etc

Challenges → Dynamic Topology [less trustable]

→ Security - [Limited] → security attacks

→ Bandwidth [Limited] → low capacity [effect of multiple access interference cond" is very low]

→ Energy [Constrained]

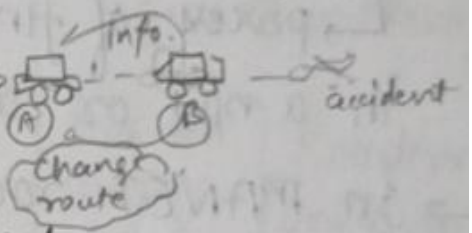
→ Routing [Difficult] [due to dynamic topology some nodes changes their position which affect the routing table]

Applications → Battlefield → war zones.
It takes less time & infra.

→ Sensor network [consist of multiple detec" sta" called sensor nodes, each of which is small, light weight and portable]

→ VANET → (Vehicle Adhoc Network) → vehicles can communicate each other to clear the traffic.

→ PAN → Personal area n/w
[one person share to other using one n/w]



Applications of Adhoc Wireless N/w

Infrastructureless → Easy to establish
→ cheap
→ Anywhere anytime.

(i) Military opera" → remote sensing

(ii) Collaborative work

(iii) Environ. app" → weather cond", forest-fire
→ Tsunami

(iv) Crisis condi" → flood, earthquake.

(v) Medical Applica" → Monitor
→ diagnosis

Issues in Adhoc - Wireless N/w

→ No fixed topology → Routing → Route acquisition delay
→ Reconfiguration of route

∴ Battery Powered Devices { Sensor nodes → Transmission Power
→ Battery monitoring

→ Security → no secure node
no secure protocols

→ Quality of Service → Some loss of data packets

Routing in MANET →

↳ process of finding the best path for traffic in a n/w or across multiple n/w.

→ In MANET routing is difficult than normal n/w due to non-fixed infrastructure and rapid change in topology.
due to node mobility

Routing protocol should follow the follow—

→ Reliability [packet will surely reach to destination]
→ Least Cost in routing traffic in n/w
→ Max.- throughput. → min. ideal time for nodes.
Each node should do work.

→ If any host demands for the route, they must have quick access.

Routing Classification

Proactive

→ Route is determined in advance.

→ Also called Table Driven Routing

→ Low N/w Mobility

→ High Control Traffic

Adv →

- Low Route Latency
- State Info^n (of each route)
- QOS Guarantee. (Quality of Service)

Disadv -

- More overhead
- Periodic update is needed.

Ex- DSDV, GRS, Fish-eye state.

Reactive

Route is determined only when needed.

High

Low

Adv → (no periodic update)

- Less overhead
- Scalability is good.

Disadv - diff to find the route

- Route Latency is high.
- Route caching can be reduced.

Ex- DSR, AODV, Locn Aided routing

Hybrid

Combination of Proactive and Reactive

Very High.

Lower than other two types.

Near by Node } Proactive, information is stored

Ex- Zonal Routing

Far away Nodes } Reactive only on need basis

Adv → Requires less memory & processing power.

Disadv → If border nodes move away, re-establish path takes long time.

Types of Adhoc Routing Protocols →

① Based on Info° Update

- **Proactive Routing** (Table-Driven Routing)
  - → Each node maintains a routing table.
  - Ex → DSDV, STAP
- **Reactive Routing** (On-demand Routing) — obtain necessary path when req.
  - → no node maintains a routing table
  - Ex → DSR, AODV
- **Hybrid Routing**
  - Combina° of both n/w is divided into zone.
  - Ex → CEDAR, ZRP.

② Based on Temporal Info for routing

- **Past History**
  - Ex → DSDV, AODV
- **Future**
  - Ex → LBR

③ Based on Topology Info

- **Flat**
  - Ex DSR, AODV
- **Hierarchial**
  - → CGSR

④ Based on Utiliza° of Specific Resources

Ex → Flooding, Geographical & Power aware.

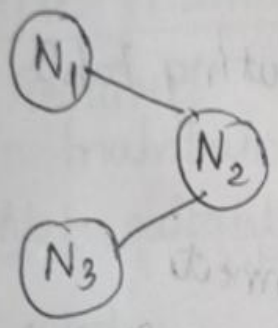
Proactive Routing Protocols -

(i) Destina" Sequenced Distance Vector Routing (DSDV)

In this each node keeps record of route info" in the form of routing table.

Table consist of → Destina" ID
→ Next Node
→ Distance (No. of Hops)
→ Seq. No.

Route Broadcast msg - Dest. node
→ Next hop
→ Recent seq. no
→ Distance.



Routing Table of N_1

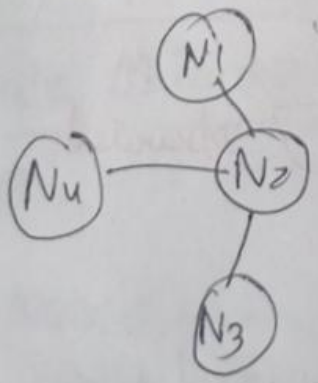
Dest.	Next node	dist.	Seq. No.
N_2	N_2	1	14
N_3	N_2	2	18

Each node exchanges its updated routing table with each other.

Updates

Full Dump
Entire routing table is sent to neighbour

Incremental updates
→ Only entries that are changed are exchanged.



Routing Table of N_1

Dest	Next node	dist	seq no.
N_2	N_2	1	14
N_3	N_2	2	18
N_4	N_2	2	22

Table Maintenance in DSDV →

(i) Each node receives the route info with most recent seq. no. from other nodes and updates its table.

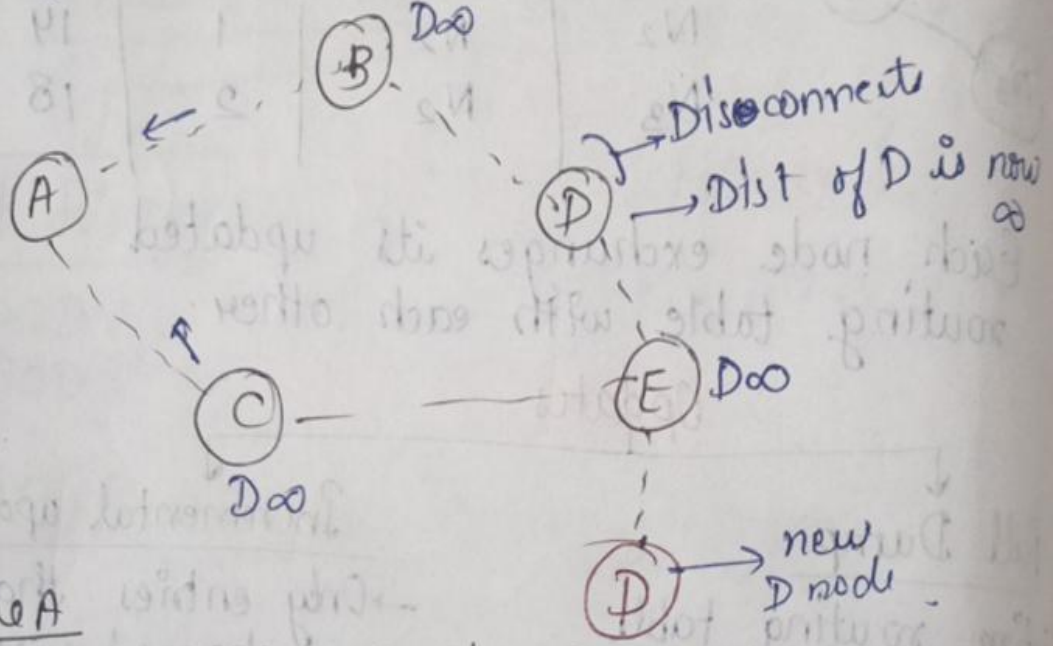
(ii) Node looks at its routing table in order to determine shortest path to reach all the destination.

(iii) Each node constructs another routing table based on shortest path info.

(iv) New Routing table will be broadcast to its neighbours.

(v) Neighbour nodes updates its routing table.

Ex



Node A

Dest	Next hop	Dist	Seq. no.	
B	B	1	340	
C	C	1	164	
D	B	2	115	Discarded
E	C	2	90	
D	C	3	124	
				new joined

(iii) Wireless Routing Protocol —

→ Another ex. of Proactive Routing
→ Similar to DSDV
→ Here, each node maintains four tables

① Distance Table → distance
→ Penultimate node

② Routing Table → → shortest dis, predecessor node, successor node, cost

③ Link cost Table → cost of the destination

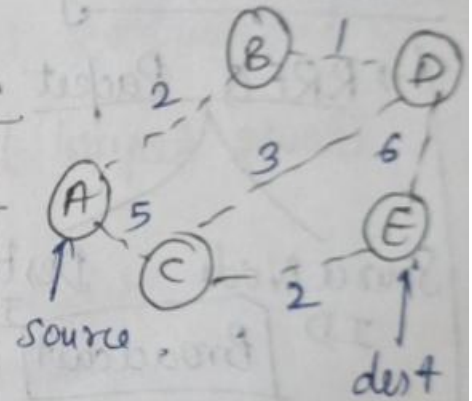
④ Message Retransmission List → Every update msg that needs to be retransmitted

Table Maintenance →

→ Requires more memory & processing power to maintain accurate info about nodes in n/w.
→ Not suitable for large n/w with high mobility

Ex: ~~Node~~ Routing table of node 'A' with dest. 'E'

Node ID	Next hop	Predecessor	Cost
A	C	C	7
B	D	C	6
C	E	E	2
D	C	C	5
E	E	E	0



Route Maintenance → During ~~like~~ link break, the node which detects like breakage will send an update msg.
↳ cost of broken link = ∞

→ NODES receiving the update msg will update its routing table

Reactive Routing Protocol →

Also k/a On-demand Routing Protocols.

Dynamic Source Routing (DSR) Protocol →

→ Discovers the route b/w source and destination when required

→ Opera" is based on Source Routing (sender knows the complete path)

→ Intermediate nodes do not maintain routing info" to route the packets to the destina"

→ Less n/w overhead as the no. of msg exchanges b/w nodes is very low.

Phases of DSR Protocol

Route Discovery

→ RREQ Packet (Route Request)

Source Node ID | Destina" Node ID | Broadcast

→ RREP Packet (Route Reply)

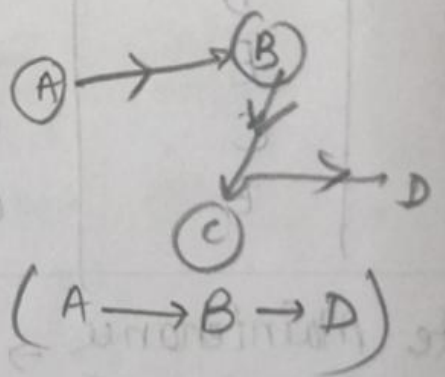
Sender | Path | Dest~

→ Unicast

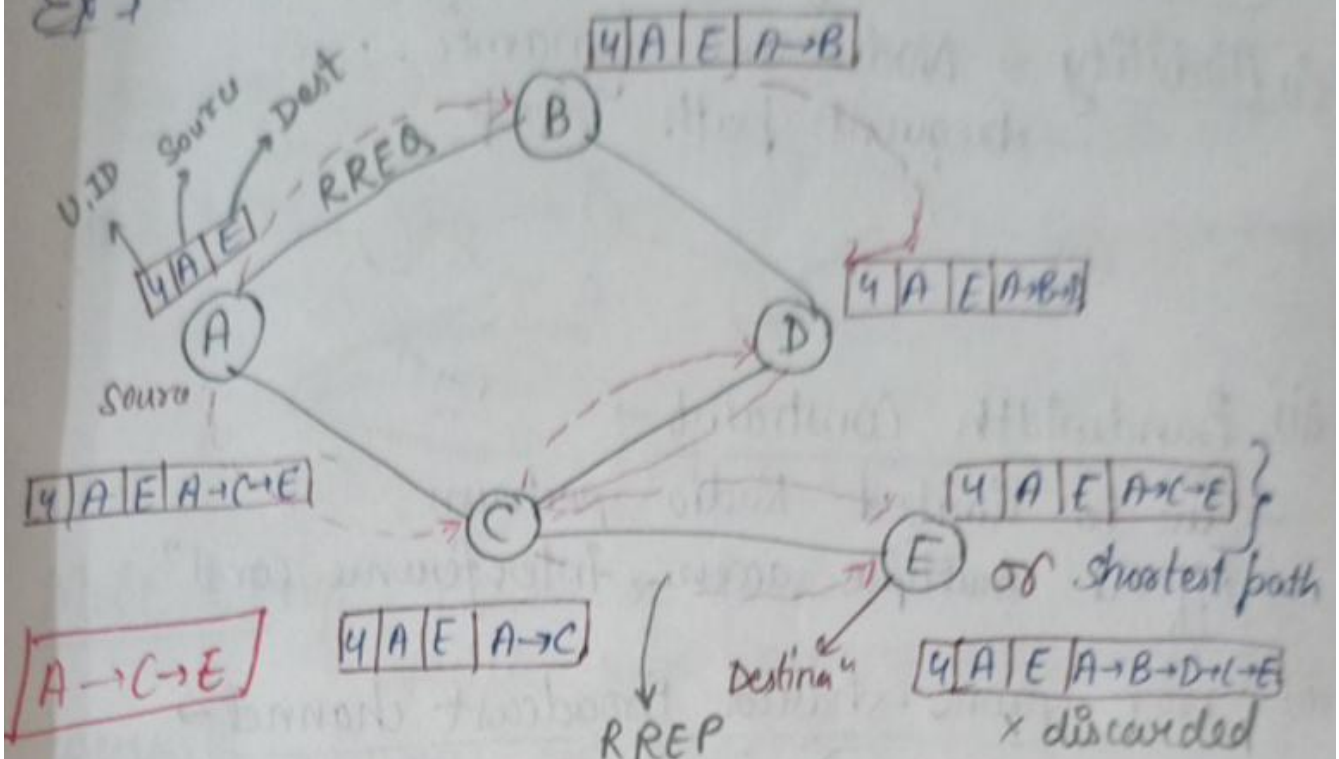
Route Maintenance

→ RERR msg (Route error)

→ Route Cache stores the path



Ex →



Routing Protocols –

Routing is the process of establishing a path b/w the the sender and receiver node for transmitting the packet along the path.

→ Routing protocol will find best optimum path
– Shortest path.

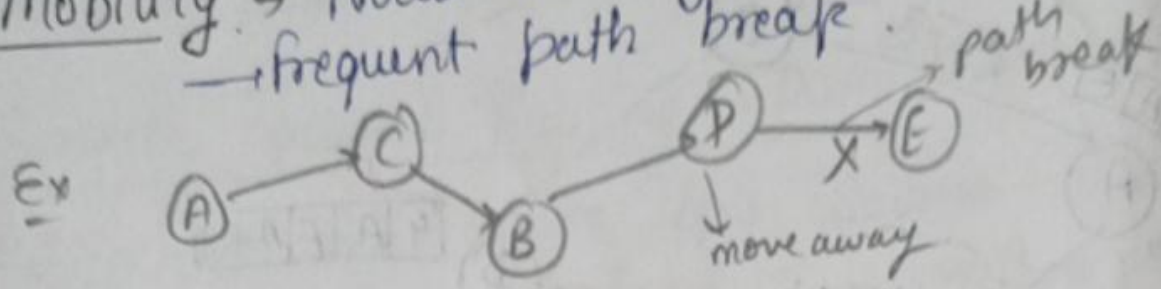
Design Constraints –

(i) Mobility of nodes
(ii) Dynamic topology
(iii) No Centralised infrastructure
(iv) Bandwidth
(v) Energy
(vi) End to end constraints.

Characteristics →
- Fully distributed
- Adaptive towards frequent changes
- Route computation and maintenance must involve min no. of nodes.
- Packet collision must be minimum

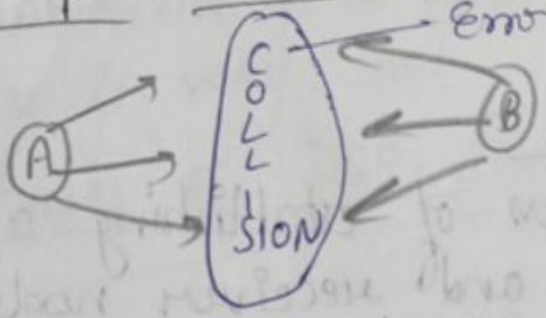
Issues in Designing Routing Protocols

(i) Mobility → Node are dynamic.
→ frequent path break.

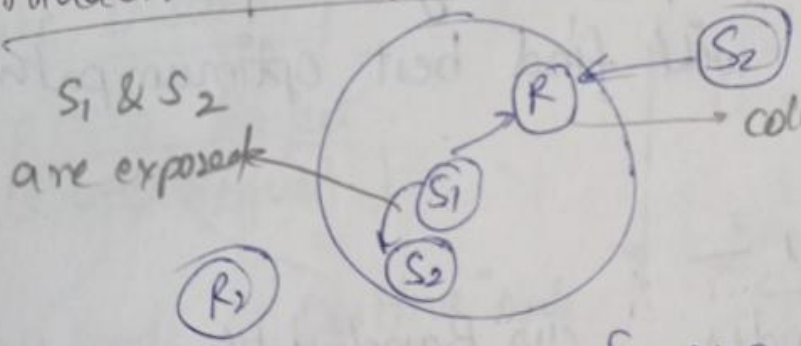


(ii) Bandwidth Constraint →
→ due to limited Radio spectrum.
→ Affecti multiple access, interference cond".

(iii) Error-prone shared Broadcast channel →



(iv) Hidden and exposed Terminal Problem →

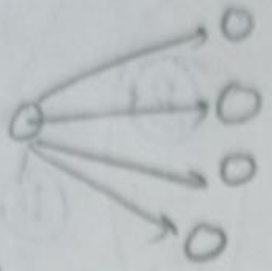


(v) Resource Contraints - • Sensor nodes
→ limited Battery, Processing power, memory and energy.

(vi) Security Issue - No centralised Secure server.

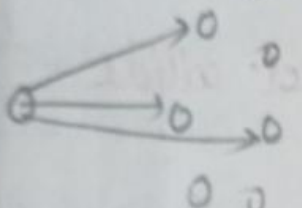
Unit - II

Broadcasting → It is the process in which one node sends a packet to all other nodes in the n/w.



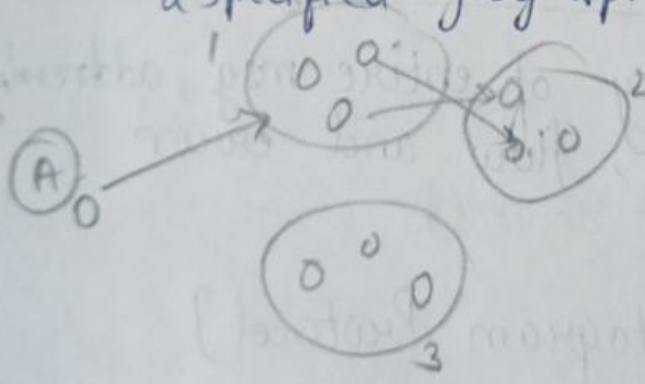
→ no need for grp mngt
→ less secure
→ More traffic
→ Slower.

Multicasting → Process of transmitting info. to specific users among all available users. → Packets are transmitted to some of the devices in the n/w



→ one to many or many to many.
→ Requires grp mngmt
→ more secure
→ less traffic → faster.

Geocasting → A technique of delivering data packets to a grp of nodes located in a specified geographical area.



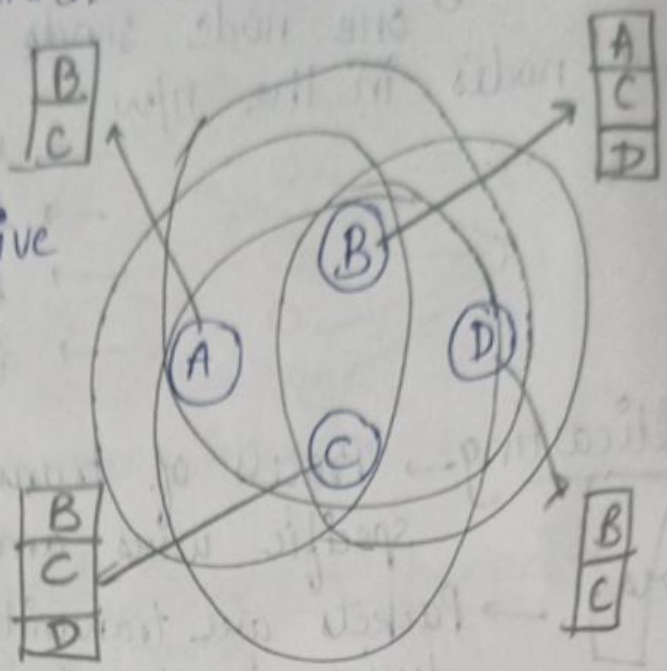
→ Country to country
→ goal is to enhance the success rate and decrease the hop ~~content~~ count & flooding rate.

Broadcasting Storm prob → In MANET, due to host mobility, such oprn are expected to be executed more frequently (like finding route, paging a host etc).
Beco2 radio signals are likely to overlap with others. In a geographical area, a straightforward broadcasting

by flooding is usually very costly, and will result in serious redundancy, contention and collision to which we call the broadcast storm prob.

Case 1 →

- Node A will receive same copy from B and C.
- Node B and C will receive same from D.



Case 2 → • If node B and C broadcast at the same time. → Packet collide

• If Node B and C broadcast at diff. time. → Redundant msg.

Transport Layer and Security Protocols →

End-to-end delivery of entire msg, addressing, reliable delivery, flow and error control. [Congestion control]

→ UDP → [User Datagram Protocol]
- → connectionless
- → Unreliable.

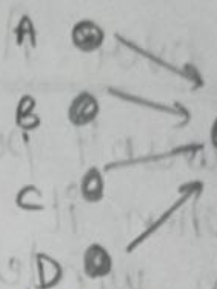
TCP → [Transport Control Protocol]
- → connection oriented
- → Reliable.

Charac... of Wireless N/w which can affect TCP Transport layer protocol →

→ Limited Bandwidth
→ High error rate
→ Mobility of nodes
→ Power consumption

Issues in Designing Transport layer Protocol-

- **Induced Traffic** → Decrease Throughput



- **Power and Bandwidth Constraints** →
  → Available resources should be used efficiently.
- **Throughput Unfairness** → Throughput / delay
  → fair share of throughput across contending flows.
- **Misinterpretation of Congestion** →
  → Hidden, exposed terminal prob.
  → Affect Transport layer Protocol.
- **Dynamic Topology** → Mobility of nodes.

Design Goals of Transport layer Protocol →

(i) Maximize throughput per connection.
(ii) Provide fairness across competing flows
(iii) Reduced connection maintenance overheads.
(iv) Scalable.

(v) Should Provide both reliable and unreliable connection.
conn^n oriented
connectionless.

(vi) Should be able to adapt to the mobility and change in topology.

(vii) Resources must be used efficiently.
bandwidth Power

TCP over Adhoc Wireless Network :-

TCP doesn't perform well when it is used in wireless adhoc n/w →

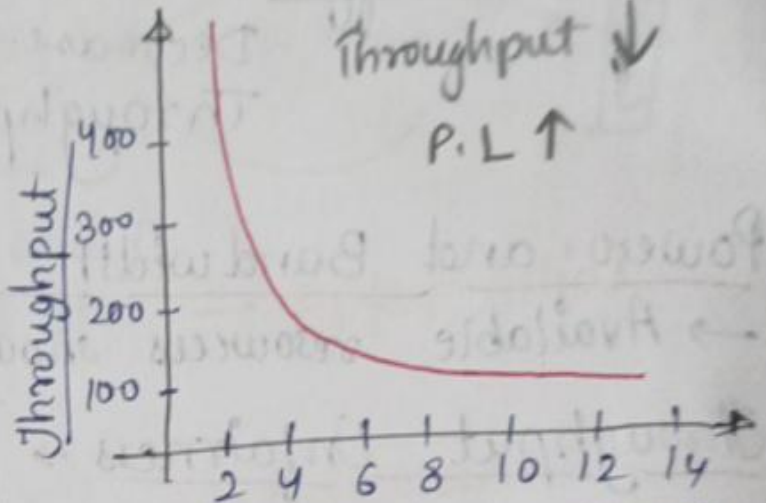
(i) Misinterpretation of packet loss.

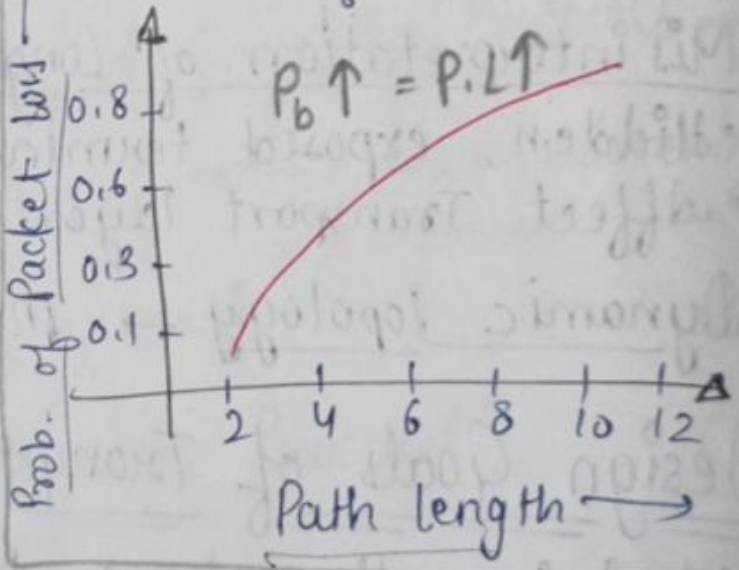
(ii) Frequent path breaks

(iii) Effect of (Path length ↑) = Throughput ↓

(iv) Misinterpretation of congestion window

(v) Asymmetric ~~link~~ link behaviour.





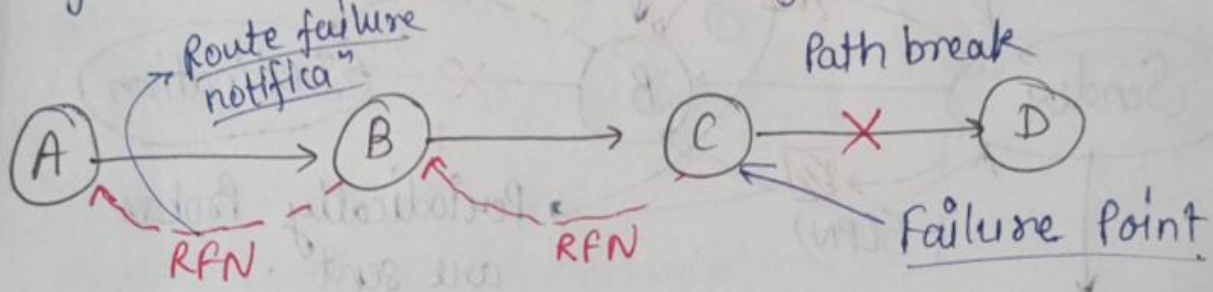
Classification of Transport layer solutions →

- TCP over Adhoc Wireless network
  - Split Approach
    - Split TCP
  - End-to end Approach
    - TCP-F
    - TCP-ELFN
    - ATCP
    - TCP-BUS.
- Other Transport layer Protocols
  - ACTP
  - ATP

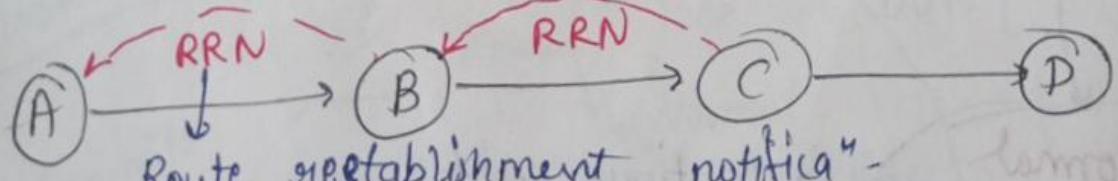
TCP-F [Feedback-based TCP)

→ Feedback-based approach

→ Objective is to reduce throughput degradation (It was the failure of TCP)



→ A and B will remove broken path information from routing table.



→ A and B will add path to D in the routing table.

Adv. of TCP-F :→ → RFN (Path break)

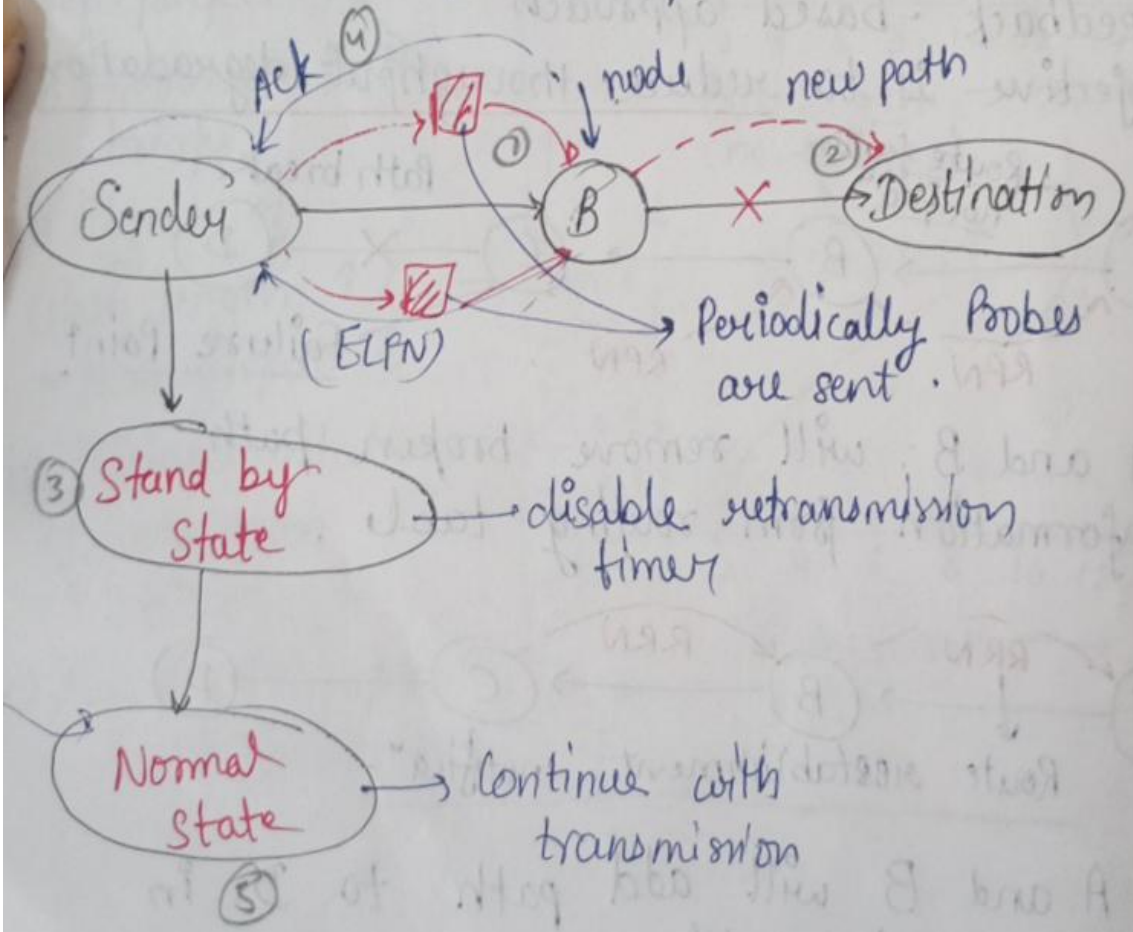
(i) Simple feedback mechanism → RRN (Path re-established)

(ii) Good congestion Control mechanism.

Disadv.→ • Requires modifica" to existing TCP libraries.

TCP-ELFN [TCP with Explicit link Failure Notification]→

- It is mainly used to improve the performance of TCP in adhoc wireless N/w.
- (ELFN) packet is generated by the node who detects a path break.



Transmission of ELFN to sender

By transmitting DUR msg [Destination unreachable]

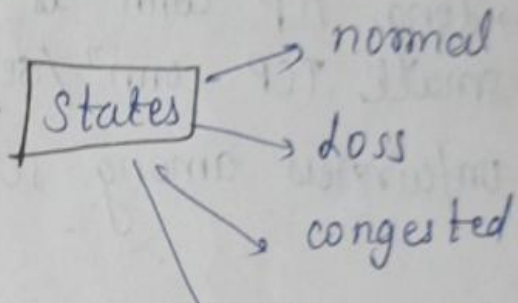
Adding ELFN msg with route error packet

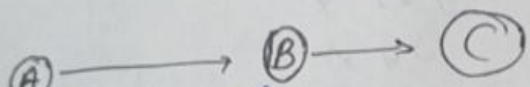
Adv → TCP performance by decoupling path break info" from congestion info".

Adhoc TCP :→ (ATCP) operation is based on the feedback mechanism

Sender can change its state due to any of the following →

(i) Persist
(ii) Congestion Control
(iii) Retransmit

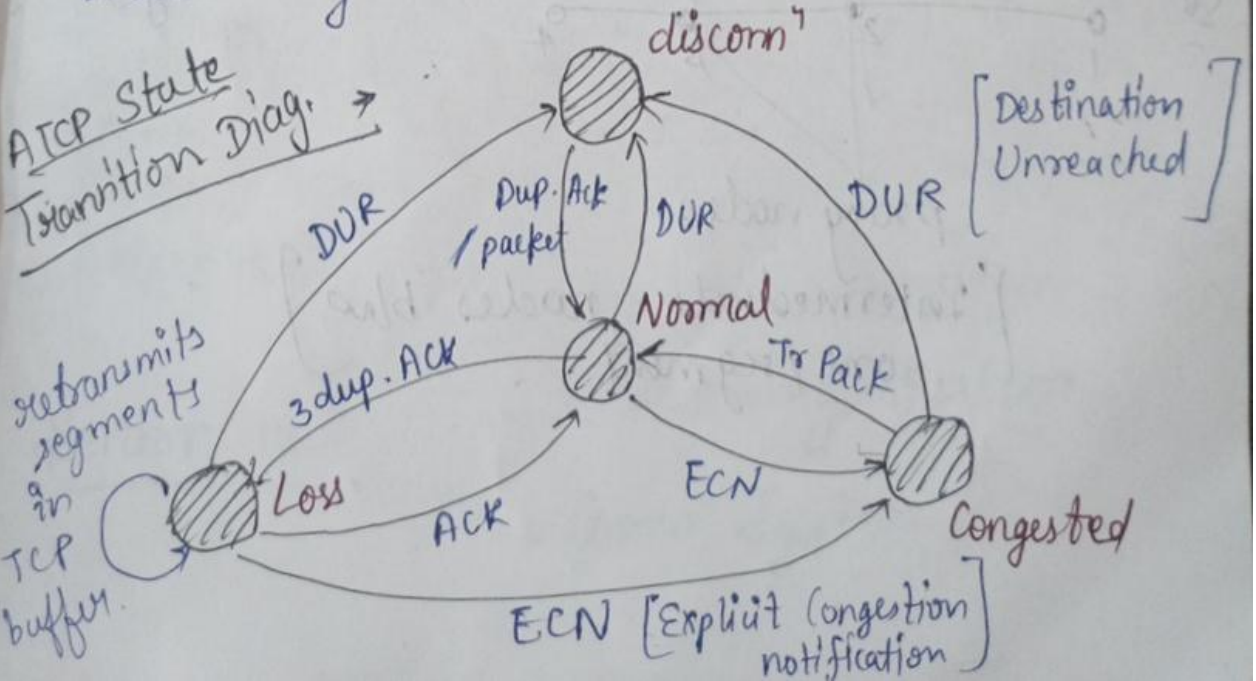




N/w is partitioned

State to persist and avoids any retransmission.

ATCP State Transition Diag. →



Adv. of ATCP →

→ Maintain the end-to end semantics of TCP
→ Compatible with traditional TCP

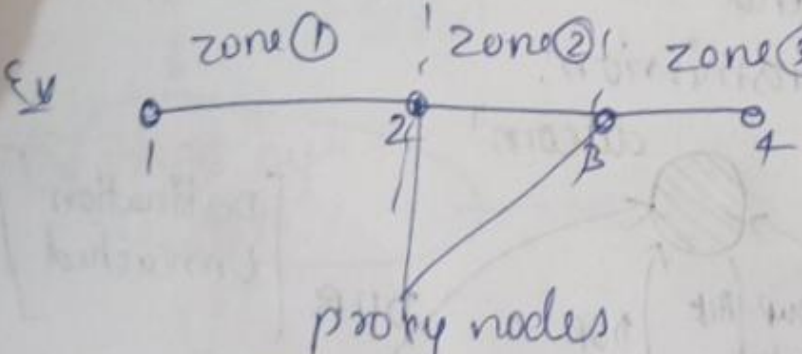
Disadv. of ATCP →

→ Dependency on n/w layer protocol.
→ Change in interface function.

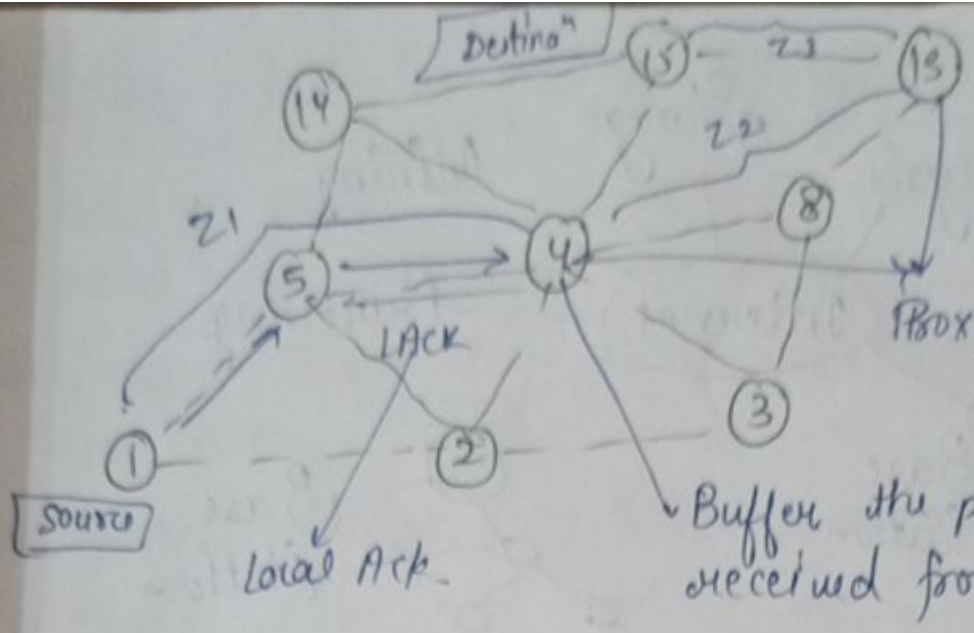
SPLIT TCP → (STCP)

Improves the performance of TCP in adhoc wireless network (degradation of throughput due to path length).
→ long TCP conn" is separated into several small TCP conn"/segments.
unfairness among session { S1 ✓, S2 ✓, S3 ✗, S4 ✗

Objectives of Transport layer → congestion control
→ End-to-end reliability



[Intermediate nodes b/w zone/segment]



Adv → ↑ throughput, Improved fairness, less impact of mobility

Disadv → Existing TCP needs modifica". → end-to-end com" is not there.

Unit - III

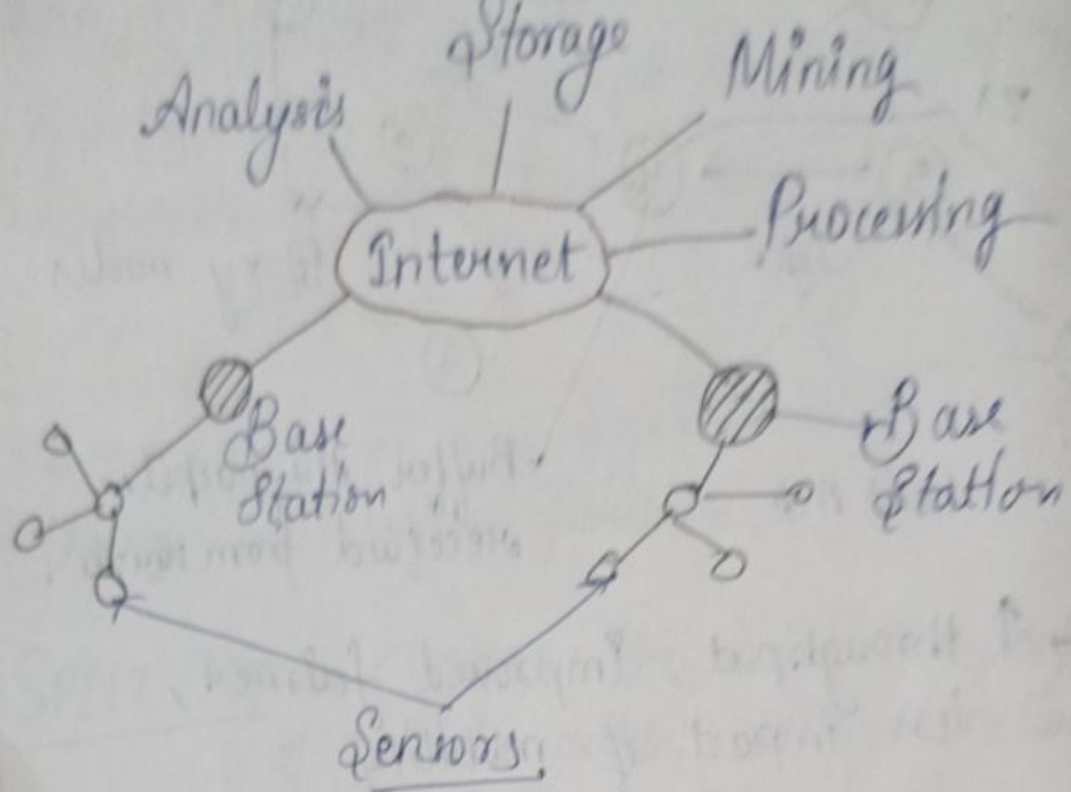
Wireless Sensor Networks →

Phy. Quantity → (Sensor) → Observable qty.

→ Sensor n/w are highly distributed → adhoc manner, lightweight nodes, dployed in large no. to monitor the environment or system.

→ Sensor nodes are fitted with on-board processor.

Sensor node → Sensor Subsystem
→ Processing System
→ Comm" System.



Applications →

(i) Battlefield → Surveilance & monitoring
(ii) Air Pressure, Temp, Humidity
(iii) Noise level
(iv) Patient diagnosis & monitoring
(v) Agriculture.

Challenges —

(i) Scalability → N/w ↑ Throughput ↓
(ii) QOS
(iii) Energy Efficiency
(iv) Security.

Adhoc Wireless N/w V/s Sensor N/w →

(i) No. of nodes in sensor n/w can be more as compared to adhoc n/w.

(ii) Sensor Nodes are more prone to failure and energy drain.

(iii) Sensor Nodes → Data Centric

(iv) Adhoc N/w → Add. Centric

(v) Most of the adhoc n/w routing protocols can't be implemented to sensor n/w.

Issues and Challenges in Designing Sensor N/w →

(i) No Regular topology

(ii) Infrastructure less.

(iii) Resource Constraints → Energy, Bandwidth.

(iv) Hardware should be energy efficient
↳ microcontroller.

(v) Security Issues → Enemy territory
→ No central tower.

(vi) Adaptible to changing connectivity

(vii) Synchronization.

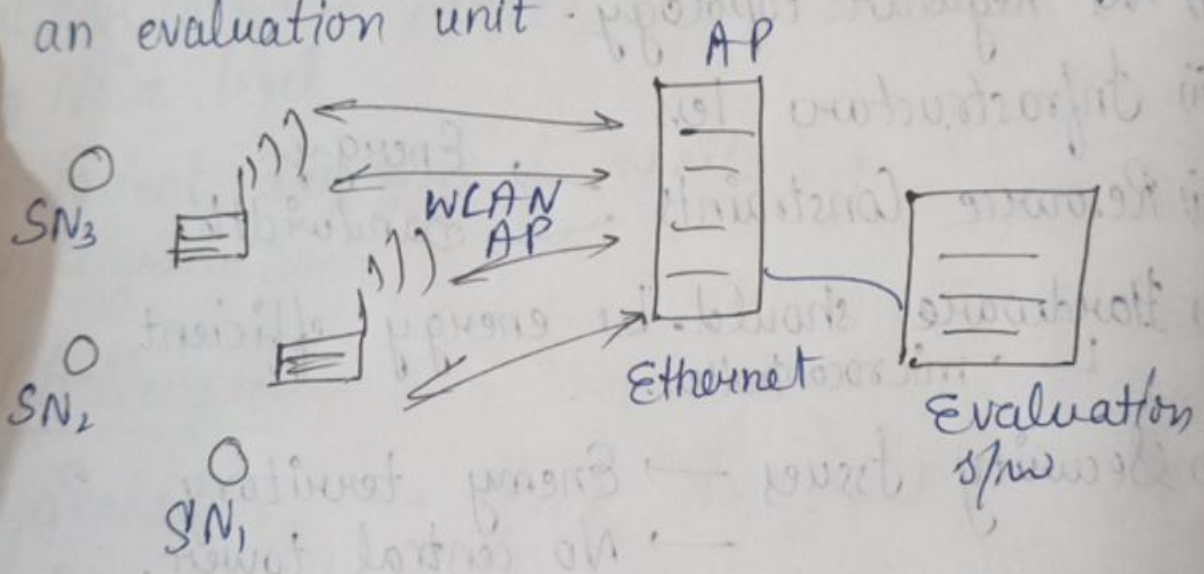
Components of WSN →

(i) Sensors → They capture the measured variable in a data acquisition n/w. For further processing sensor signal is converted into electrical signal.

(ii) Wireless Sensor nodes or Radio nodes – They receive the sensor data from sensors.

(iii) WLAN Access Point → Receives sensor data which are transferred by sensor nodes wirelessly.

(iv) Evaluation s/w → For any data analysis, WLAN access point is connected to an evaluation unit.



Components of a Wireless Sensor Node –

(i) Microcontroller → This is a computer on a chip which is very small in size.
→ Capable of doing powerful tasks including controlling the func" of other devices connecting to it.

Microcontroller → Microprocessor
→ RAM Memory
→ Associated Peripherals.

(ii) Transreceiver → This is transmitter - receiver that is used for comm" purposes to send and receive data and commands

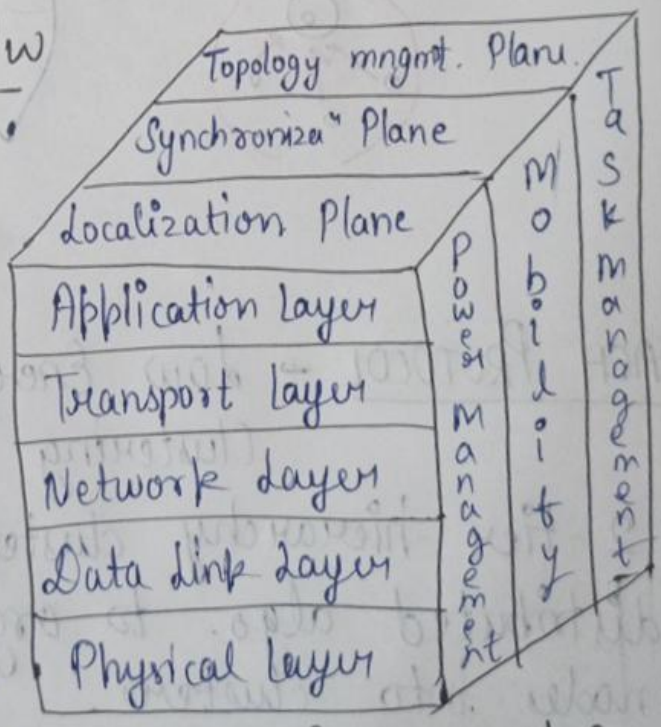
(iii) External Memory → (WSN) nodes usually use flash memory
- Small in size
- Reasonal Storage capacity

(iv) Power Source → Power is stored in the form of batteries.

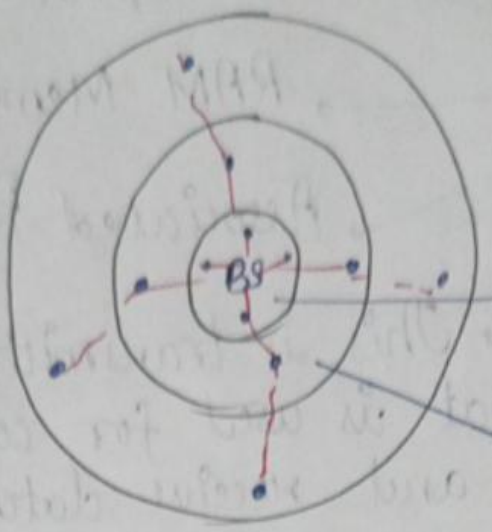
Sensor N/W Architecture →

(i) Layered N/W Arch.

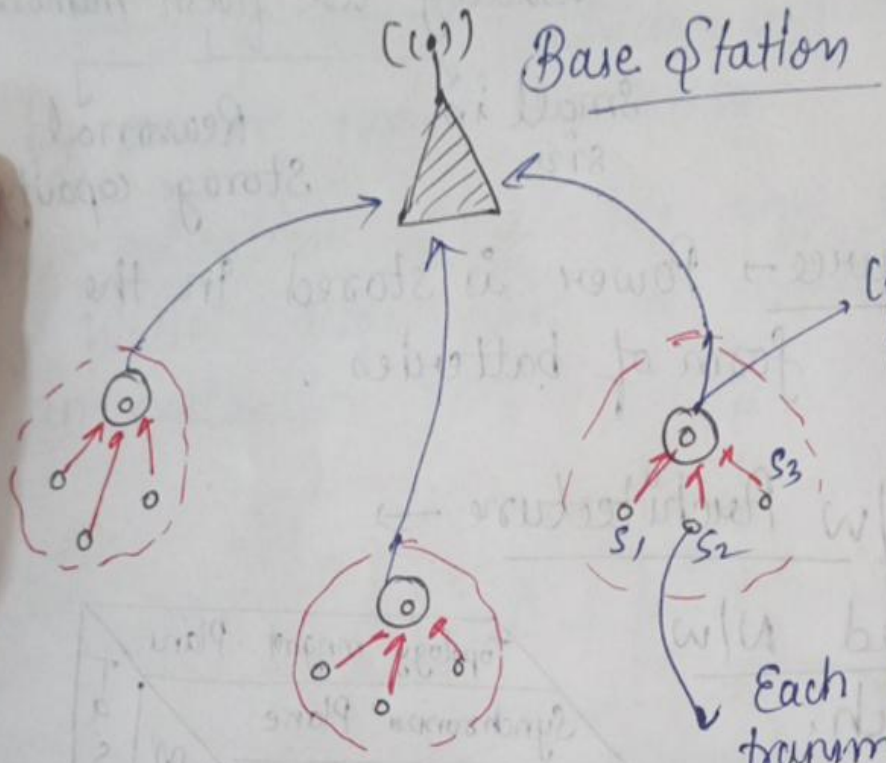
It includes five layers and three cross layers.
→ Scalable, fault tolerance, Power consumption is less.



Sensor N/W Protocol Task



(ii) Clustered N/w Architecture →



LEACH PROTOCOL = Low Energy Adapting Clustering Hierarchy

→ 2-tier hierarchy clustering architecture.
→ distributed algo. to organize the sensor nodes into clusters.
→ Cluster head nodes create TDMA Schedules

→ Energy Efficiency = Data Fusion

LEACH

- Set up
- Steady
  - Transmission of data.