UNIT 3 - ADHOC and WSN

Infrastructure network and Infrastructure less wireless networks.

Wireless networks can operate in two primary modes: infrastructure and ad-hoc (infrastructure-less).

1) Infrastructure network - It is a wireless network where devices communicate through a central access point (AP), such as a wireless router or Base station. The AP manages all network communication, providing a stable & secure connection for all devices on the network.

2) Adhoc Network - It is a wireless network where devices communicate directly with each other without any central AP. Each device acts as both a host and a router, allowing for quick & temporary peer-to-peer connections.

Feature	Infrastructure Network	Ad-hoc network
Communication	Through AP.	Directly between devices
Central Control	Yes (AP manages network)	No (decentralized)
Routing is	Managed by AP	Managed by individual nodes
Security	More options, stronger	Limited, often weaker.
Performance	Faster, more reliable	Slower, less reliable.
Setup	Complex, requires infra	Simple, quick, no infra needed
Applications	Home / office, Wifi, cellular, hotspots	Temporary network, military, emergencies.
Range	Determined by no. of AP's	Limited to device-to-device range

Issues in Adhoc wireless network.

1) Medium Access Control (MAC): Distributed operation, hidden/exposed terminal problems and synchronization.
2) Routing: Frequent path breaks due to node mobility, bandwidth constraints and error prone channels.
3) Security: Vulnerable to DoS attack, energy depletion and buffer overflow.
4) Quality of Service (QoS): Difficulty in resource reservation & handling traffic
5) Energy Management: Limited battery life for mobile nodes.
6) Dynamic Topology: Nodes can move randomly → frequent route changes
7) Multicasting: Robustness, Efficiency and Control overhead.
8) Addressing challenges: Absence of centralized coordination, security risks (MIME)
9) Service discovery challenges: Lack of infra (no centralized directory), Overhead and efficiency, latency and Accuracy

Adhoc Network MAC layer: Design issues

1) Bandwidth Efficiency: The goal is to maximize the ratio of bandwidth used for actual data transmission to the total available bandwidth. Inefficient use leads to increased collisions, retransmissions, and waste energy.

2) Quality of service (QoS) support: Providing QoS is difficult due to the high mobility of nodes and the lack of centralized control. Ensuring reliable support for time-critical and multimedia traffic is challenging.

3) Synchronization: Achieving & maintaining synchronization in a distributed, mobile environment is complex and may require periodic exchange of packets.

4) Hidden and exposed terminal problem: Prevent collisions & unecessary transmission blocking.

5) Mobility: Nodes in adhoc networks are mobile, causing frequent changes in network topology. This mobility can lead to broken links, lost reservations, and need of rapid adaption.

6) Error Prone, shared wireless channel: Wireless medium is error-prone due to ~~inf~~ interference, fading and noise.

7) Distributed Coordination: no central controller; all nodes must coordinate

8) Power Constraints: Mobile nodes often operate on battery power.

9) Control Overhead: Excessive control messages can consume significant bandwidth and energy, reducing network efficiency.

Design Goals

1) Distributed operation: No central coordinator / controller; nodes coordinate among themselves
2) collision avoidance: minimize simultaneous transmission to reduce interference.
3) Energy efficiency: Save battery power for mobile nodes.
4) fairness: Ensure all nodes get fair access to the channel.
5) Scalability: work well as the network size changes.
6) Adaptability: Quickly adjust to node mobility & topology changes.
7) QoS support: Prioritize traffic based on application nodes.
8) Hidden Terminal Mitigation: Handle nodes that cannot hear each other but interfere.
9) Security: Protect against unauthorized access & attacks.
10) Efficient Channel Utilization: Maximize use of available bandwidth.
11) Support Multimedia Traffic: Handle diverse data rates and delay requirements.

Classification of MAC Protocols in adhoc wireless network

1) Contention-based Protocol:-

- A node does not make any prior resource reservation. All nodes compete for the channel. When a node wants to send data, it first checks if the channel is free. If it is, the node transmits; if not, it waits for a random time before trying again.

Examples: CSMA/CA, MACA, MACAW.

- flexible & simple, but may suffer from collisions and reduced efficiency under high load.

2) Contention based protocol with reservation mechanism :-

- Nodes compete for the channel, but only during a special reservation phase. Once a node successfully reserves bandwidth, it can transmit data without further contention during reserved period.

- Eg. : D-PRMA, RTS/CTS.

3) Contention based protocols with scheduling mechanism :-

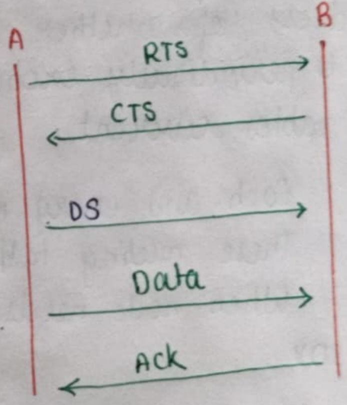
- Nodes compete for access, but a scheduling mechanism (like a queue) determines the order or timing of transmissions. This ensures fair access & can help manage energy consumption and avoid starvation.

- Eg : DPS, Non scheduling protocols.

MACAW (Multiple Access with Collision Avoidance for Wireless)

It is a MAC protocol designed for wireless ad hoc networks. MACAW extends MACA improve its ~~has~~ performance.

Working :



1) 5 step Handshake : MACAW uses a specific sequence of control messages before and after sending data to avoid collisions and inform nearby nodes.

RTS (Request to send) - Sender asks receiver for permissions.

CTS (Clear to send) - receiver responds.

DS (Data sending) - The sender announces the size and duration of upcoming data transmission, so other nearby devices know how long the channel will be busy.

DATA - The actual data is transmitted

ACK (Acknowledgement) - Receiver confirms successful receipt of the data.

2) Non-Persistent Slotted Access - After the channel is busy, all nodes wait a random time after the start of next time slot before trying to send an RTS. This randomness gives all nodes a fair chance to access the channel.

3) Improved Backoff Algorithm - MACAW increases the waiting time multiplicatively after collisions and decreases it linearly after successful transmission

4) Addresses Wireless Challenges - MACAW's design tackles hidden / exposed terminal problems and improves fairness & efficiency.

Adhoc Network Routing Layer

Routing layer is responsible for finding and maintaining routes between nodes in a network. Since nodes move and there is no fixed architecture, routing in Adhoc networks is much more challenging than in traditional network.

Issues in Designing a Routing protocol for Ad-hoc wireless ~~to~~ Networks

1) Dynamic Topology : nodes move randomly → frequent changes in network
2) Limited Bandwidth : Have lower capacity than wired networks.
3) Energy constraints : nodes rely on battery power.
4) Error-prone channels : more easily prone to errors due to fading, interference
5) Hidden & Exposed station problem - cause collisions and defer transmissions
6) Scalability : Protocol should handle growing no. of nodes.
7) Route ~~Maintain~~ Maintenance - Route breakages must be detected and repair fast.

Classification of Routing Protocols

1) Proactive (Table-driven) Routing Protocol -

It maitain up-to-date routes to all possible destinations at all times, regardless of whether data needs to be sent. Each node keeps a routing table & periodically exchanges routing info with neighbours to keep these tables current.

Working : Each and every node has a routing table
These routing tables are updated regularly when network changes occur.
When node needs data to send, it can lookup the route in its table.

Eg. DSDV

2) Reactive (On-demand) Routing Protocols -

Creates route only when needed. When a node wants to send data to a destination, it initiates a route discovery process. Routes are maintained as long as they are needed.

Working : No periodic route updates; instead routes are discovered & established on demand.
When communication is needed, the source node sends route req.
The route is established when, route reply is received & data transmission can begin.
If route breaks, a new discovery process is started.

Eg. AODV, DSR

3) Hybrid Routing Protocols -

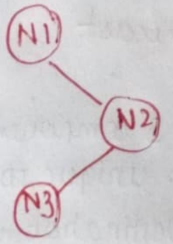
Combines strengths of proactive and reactive approaches. Typically, the network is divided into zones or clusters. Within each zones, routes are maintained proactively; betn zones, routes & discovered on demand. Eg. ZRP

DSDV (Destination- Sequenced Distance Vector)

- In this each node keeps record of rowe info inthe form of routing table.

Table consist of : Destination ID , next node, distance (no. of hops), seq. no.

Routing broadcast msg : Destination node, next hop, Rececent seq. no, distance



Routing table of N1

Dest	next node	distance	sequence no.
N2	N2	1	14 (randomeg)
N3	N2	2	18

- Each node exchanges its updated routing table with each other.

updates → Full Dump - Entire routing table is sent to neighbour.
updates → Incremental Dump - Only entries that changed are exchanged

Table ~~maintainance~~ maintenance

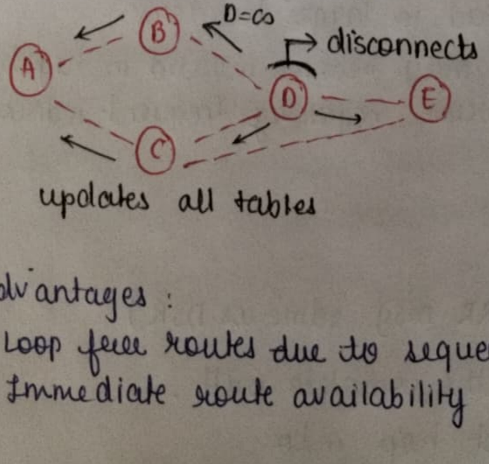
i) Each node receives the route info with most recent seq. no from other nodes and updates its table.

ii) Nodes looks at its routing table in order to determine shortest path to reach all the destinations.

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.



updates all tables

Node A

Dest.	next hop	distance	seq. no
B	B	1	340
C	C	1	164
D	B or C	2	125 } discarded
E	C	2	160

Advantages :

1) Loop feree routes due to sequence nos.
2) Immediate route availability

Disadvantages :

1) Regular updates consume bandwidth & battery.
2) Not suitable for highly dynamic or large networks due to overhead.

DSR (Dynamic Source Routing)

- Discovers the route between source and destination when required.
- Operation is based on Source Routing (source knows the complete path)
- Intermediate nodes do not maintain routing info to route the packes to the destination.
- less network overhead as the no. of message exchange betn nodes is very low

Phases of DSR Protocol

Route Discovery - RREQ Packet (Route req.) → Source Node ID → Destination Node ID — Broadcast

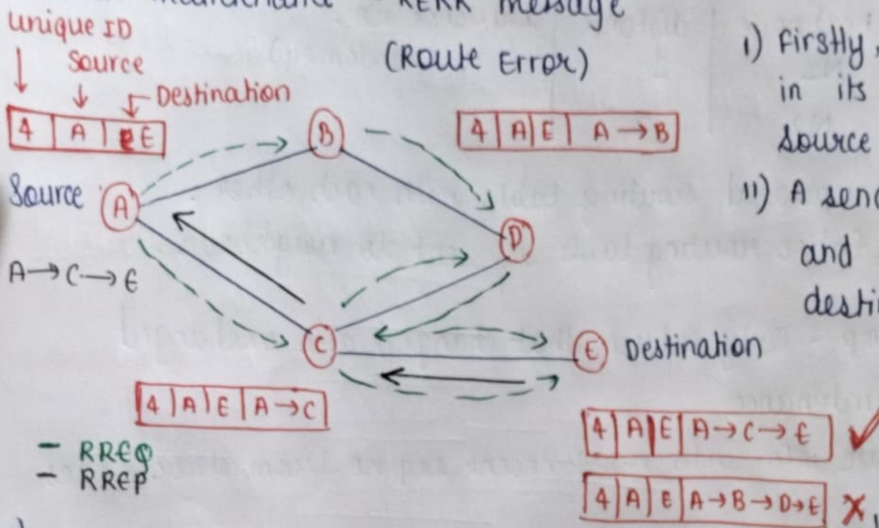
- RREP Packet (Route Reply) = Destination sends path to sender — Unicast

Route maintenance - RERR message (Route Error)

i) Firstly, Source has 3 component in its packet info : uniqeue ID, Source node and Destination node

ii) A sends RREQ to neighbours, and this continues unitil destination is reached

iii) Simultaneously, the table gets updated ~~oby~~ by adding its route.



iv) Shortest path /route is choosen

v) Once, destination route is fixed, the info. is send back to source node with all route node ie 4 | A | E | A → C → E is send back to A (by RREP)

Advantages :

1) Source Routing
2) No periodic updates needed
3) Low overhead
4) Supports unidirectional links

Disadvantages :

1) Header Overhead - carry full route in each packet can lead to large headers.
2) Cached routes may become invalid in highly mobile scenarios, requiring frequent rediscovery

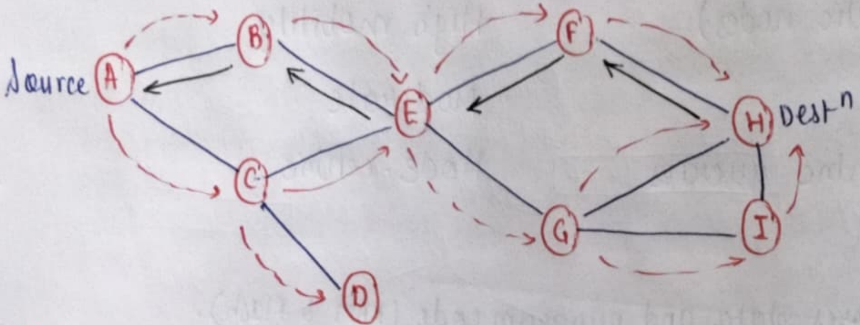
AODV (Adhoc- On Demand Distance Vector)

Operates on 2 phases → Route Discovery
→ Route Maintenance (RERR msg same as DSR)

- Unlike DSR, AODV source node will not carry the complete path.
- Each node only knows its previous and next hop info.
- Each node maintains Route cache.

Route Discovery - (RREQ) : Source node ID
Destination node ID
Recent seq. no.
Broadcast ID
Hop Count
TTL (Time To Live)

- Source send RREQ to neighbouring nodes ; this continues until destination is reached
- Once, route is selected ; desination node sends RREP to source node. And all nodes in path updates route cache.



- RREQ
- RREP

Route 1 : A → B → E → F → H
2 : A → C → E → G → H
3 : A → C → E → G → I → H

Only difference betn AODV and DSR is that DSR source node knows the complete path of the network (ie route) and AODV source node knows only the next hop information.

Advantages :
1) Efficient use of bandwidth (no constant updates).
2) Adapts quickly to changing network topologies.
3) Ensures fresh & loop free routes using sequence numbers.

Disadvantages :
1) Initial route discovery can cause delays.
2) Flooding of RREQ's may cause temporary bursts of network traffic.

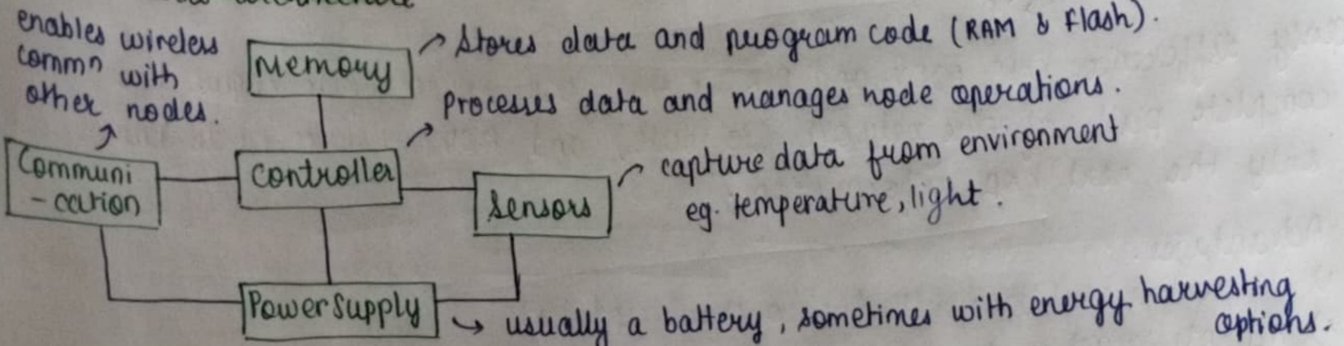
Applications of Sensor Network (WSN - Wireless Sensor Network) :
1) Environmental Monitoring - tracking climate conditions, ~~pollutions~~, natural disaster
2) Industrial Automation - monitoring machinery, energy usage and safety in factories
3) Healthcare - Patient monitoring, traffic vital signs and supporting assisted living
4) Agriculture - monitoring soil moisture, crop growth & livestock conditions.
5) Military & Security - Surveillance, battlefield monitoring and ~~illus~~ intrusion detection.
6) Smart Homes & Cities - managing lightning, temperature and energy consumption

Comparision of Sensor Network and Adhoc Wireless Network

Feature	Sensor Network	Adhoc Wireless Networks.
1) Node Count	Typically much larger	Smaller, often ten to hundreds.
2) Purpose	Sensing environment & reporting	General communication between devices.
3) Data	Many to one (towards BS)	Many to many
4) Node Capabilities	Limited processing, memory, and energy.	More powerful, often with replaceable batteries.

5) Communication	Data centric, multi-hop, often relay-based.	Peer to Peer, flexible routing
6) Energy source	Non-replaceable, non-recharable batteries common	Batteries often replaceable/ rechargeable.
7) Mobility	No (static nodes)	High mobility
8) Scalability	High	Moderate
9) Addressing	Data-centric queries	Node-centric

Sensor node architecture



enables wireless commn with other nodes.

Stores data and program code (RAM & flash).

Processes data and manages node operations.

capture data from environment eg. temperature, light.

usually a battery, sometimes with energy harvesting options.

Issues and Challenges in Designing Sensor Networks.

1) Target Coverage and Connectivity : Ensuring that all points / targets of interest are monitored by at least one sensor is a core problem in WSN. Organizing sensors into groups and scheduling their activity helps maximize surveillance quality & network lifetime, while maintaining connectivity ensures data can reach the base station.

2) Data Collection : Gathering sensed data from nodes to a central sink is a primary function of WSN. Various schemes are used, but reliability can be affected by node mobility, traffic and connectivity issues.

3) Network lifetime : Since sensor nodes have limited, often non-replenihable energy, extending the operational period of the network is a major challenge. Techniques like load balancing and efficient routing are employed to distribute energy consumption and prolong network life.

4) Data Compression : Because transmission consumes more energy than processing, compressing data before sending it helps reduce power usage and makes better use of limited bandwidth and memory.

5) Security and Privacy : WSN are highly vulnerable to various security threats (eavesdroping, jamming, node capture, dos, etc) due to their wireless nature & deployment in open environments. So, ensuring data confidentiality, integrity, authentication, and privacy is critical.

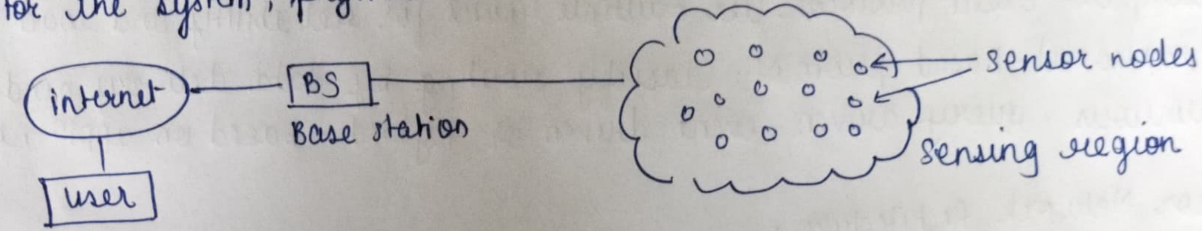
6) Synchronization : Coordinating nodes timing for accurate sensing & communication is crucial.

7) Scalability : Supporting large no. of nodes without performance loss.

8) Mobility Support : Handling movement of nodes or sinks while maintaining network functions.

Classification of sensor network protocol

What is WSN? It is infra-less wireless network that is deployed in a large no. of wireless sensors in adhoc manner that is used to monitor the system, physical or environmental conditions.



WSN routing protocols:

1) Location-Based Protocol :

How they work - use physical location of nodes to guide routing decisions.

Purpose - Calculate distances between nodes to estimate energy consumption and select energy-efficient paths.

key features - Enable directional data forwarding & efficient route discovery.

Eg - MECN, GAF, GEAR, Span, TBF, BVGF, GeRaF, SMECN

2) Data-Centric Protocol :

How they work - focus on data itself rather than node addresses; queries are sent for specific data, and nodes with relavant data respond.

Purpose - reduce redundant transmissions by aggregating data from multiple sources before forwarding to the sink.

key feature - Energy savings through in-network data aggregation & query-based communication.

3) Hierarchical Protocol :

How they work - organize nodes into clusters, each managed by a cluster head. Regular nodes send data to their CH, which aggregates and forwards it to BS.

Purpose - Improve scalability and energy efficiency by reducing the no. of long data transmissions.

Key features - Clusters heads rotates to balance energy use; communication is often two-tiered

Eg - LEACH, TEEN, PEGASIS

4) QOS Based Protocol:
How they work - Designed to meet specific QOS requirements such as low latency, high reliability or bandwidth guarantees.
Purpose - support applications with strict performance needs
key features - Prioritize traffic, manage delays and ensure reliable delivery.
Eg. SPEED, SAR.

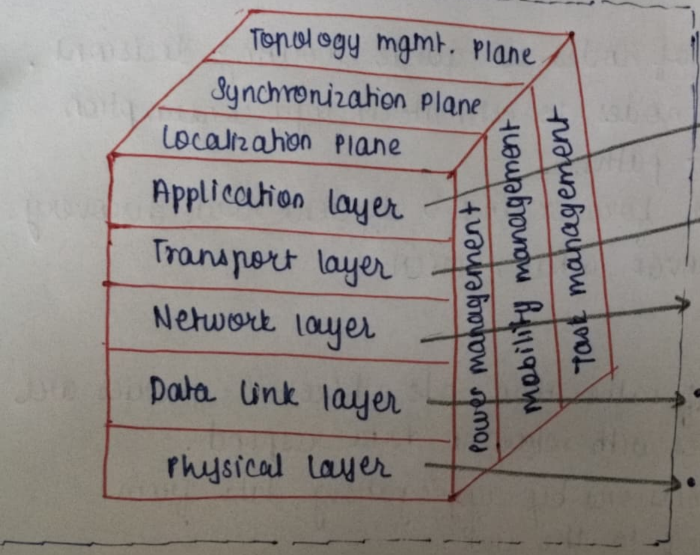
5) Mobility based Protocol: Handle dynamic routes for mobile nodes/sinks to maintain connectivity.

6) Multipath-Based protocol: Use multiple routes for reliability and load balancing

7) Operational-Based protocol: Classify routing by data delivery models - continuous, query driven, event driven or hybrid - based on appl^n needs.

Sensor Network Architecture:

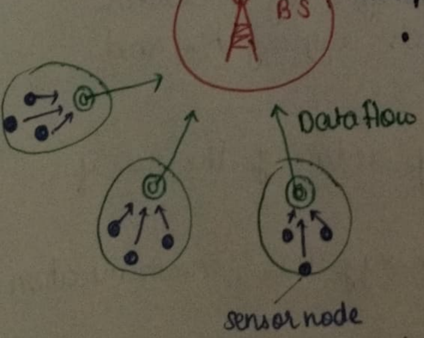
Layered Architecture: It includes 5 layers and 3 cross layers.



- Interfaces with end users/appl^n, processing and presenting data.
- Ensures reliable data delivery and manages data flow.
- Responsible for routing data from sensor nodes to BS.
- Manages data frames, error control and medium access (MAC).
- Handles transmission of raw data bits over wireless medium.

- Each layer communicates with the layers directly above and below it, following protocol stack similar to OSI model.

Clustered Architecture (LEACH Protocol)



- Grouping - Sensor nodes are divided into small groups called clusters
- Cluster head - Each cluster head has a leader called cluster head. The cluster head is chosen randomly & changes regularly so that no single node uses too much energy
- Two levels - This forms 2-tier system
- TDMA scheduling - The cluster head gives each node a time slot (using TDMA), so nodes take turns sending data.
- The cluster head combines data from its members before sending it to BS.

Clusters & cluster heads are choosen automatically by nodes themselves in distributed way. Main Goal is to use less energy and make network last longer