UNIT I

Introduction to Ad Hoc Networks

An **ad hoc network** is a decentralized wireless network that doesn't rely on fixed infrastructure like routers or access points. Devices in an ad hoc network communicate directly with each other. Such networks are often used in situations where traditional infrastructure is unavailable or impractical.

One common form of ad hoc networks is the **Mobile Ad Hoc Network (MANET)**, where mobile devices dynamically form a network without centralized administration.

Characteristics of MANETs (Mobile Ad Hoc Networks)

A **Mobile Ad Hoc Network (MANET)** is a self-configuring network of mobile devices connected by wireless links. These networks operate without any fixed infrastructure, such as routers or access points, and rely on the devices (nodes) to communicate directly or via other nodes acting as intermediaries. Here are the key characteristics of MANETs:

1. Dynamic Topology

- The network topology in a MANET is highly dynamic, as nodes are mobile and frequently join or leave the network.
- This mobility leads to constantly changing routes, requiring routing protocols that can quickly adapt to topological changes.

2. Decentralized Architecture

- MANETs do not rely on centralized infrastructure (e.g., routers or access points).
- Nodes themselves act as hosts and routers, forwarding data for others in the network.

3. Multi-hop Communication

- Direct communication is not always possible due to limited wireless range.
- Nodes forward packets for other nodes to enable communication between distant nodes, forming a **multi-hop network**.

4. Limited Bandwidth

- Wireless communication channels in MANETs have limited bandwidth compared to wired networks.
- This constraint requires efficient use of the available spectrum to minimize congestion and ensure reliable data transmission.

5. Energy Constraints

- Nodes in MANETs are typically battery-powered devices with limited energy resources.
- Energy-efficient protocols are crucial to extend the lifespan of the nodes and the overall network.

6. Scalability Challenges

- MANETs must accommodate varying numbers of nodes, from small-scale networks to large ones.
- The performance of the network may degrade as the number of nodes increases due to issues like congestion and route discovery overhead.

7. Lack of Fixed Infrastructure

- MANETs operate without any fixed infrastructure, making them suitable for deployment in remote areas, disaster zones, and military operations.
- However, this also means that all network functions, such as routing and resource allocation, must be performed collaboratively by the nodes.

8. Frequent Network Partitioning

- The dynamic movement of nodes can lead to temporary disconnections, causing the network to partition into smaller sub-networks.
- Protocols must handle these partitions and re-establish connections when nodes move back into range.

9. Security Vulnerabilities

- The lack of centralized control and open wireless medium make MANETs vulnerable to various security threats, including eavesdropping, spoofing, and denial-of-service attacks.
- Secure communication protocols are essential to protect the data and nodes.

10. Self-organization

- Nodes in MANETs are capable of organizing themselves without the need for human intervention or centralized control.
- This self-organizing capability is crucial for quick deployment in emergency or temporary scenarios.

11. Autonomous Operation

- Each node operates independently, managing its resources (e.g., power, memory, and processing).
- Nodes can enter and leave the network at will, and the network must continue to function seamlessly.

12. Variable Node Capabilities

- Nodes in a MANET may have different processing power, storage, energy capacity, and communication range.
- Protocols must account for these heterogeneities to ensure fair participation and load balancing.

13. Low Latency for Short Ranges

- Communication between nearby nodes typically has low latency due to the short wireless range.
- However, as the number of hops increases, latency may rise significantly.

14. Opportunistic Resource Utilisation

- Nodes may exploit any available resources, such as unused bandwidth or idle nodes, to enhance performance.
- Resource allocation must be efficient to maximize network throughput.

15. Support for Mobility

- MANETs are designed to support node mobility, enabling seamless communication even when devices are in motion.

- Mobility models are often used to predict and manage movement patterns for efficient routing.

Applications of MANETs

- **Military Operations**: Communication between soldiers or vehicles in a battlefield.
- **Disaster Recovery**: Establishing communication in areas affected by natural disasters.
- **Remote Monitoring**: Tracking wildlife or monitoring environmental conditions in inaccessible areas.
- **Vehicular Networks**: Enabling communication between vehicles (VANETs).
- **Smart Devices**: Facilitating communication in smart homes or IoT networks.

MANETs are versatile and highly adaptable, making them suitable for dynamic and infrastructure-less environments. However, challenges such as energy efficiency, security, and scalability must be addressed to ensure their reliability and effectiveness.

==========
==========

Applications of MANETs (Mobile Ad Hoc Networks)

MANETs are highly versatile and have a wide range of applications due to their infrastructure-less and self-configuring nature. Here are the main application areas:

1. Military Applications

- **Description**: MANETs are extensively used in military operations where a fixed infrastructure is not feasible.
- **Examples**:
    - Communication between soldiers, vehicles, and command centers on the battlefield.
    - Real-time surveillance and coordination during missions.

2. Disaster Recovery and Emergency Services

- **Description**: In disaster-affected areas where traditional communication infrastructure is damaged, MANETs provide quick and reliable communication.
- **Examples**:
    - Coordination between rescue teams during natural disasters.

    - Communication in remote areas for search-and-rescue operations.

3. Vehicular Ad Hoc Networks (VANETs)

- **Description**: MANETs are used in vehicles to form dynamic networks for intelligent transportation systems.
- **Examples**:
    - Communication between vehicles (Vehicle-to-Vehicle, V2V) for collision avoidance.
    - Vehicle-to-Infrastructure (V2I) communication for traffic management.

4. IoT and Smart Environments

- **Description**: MANETs enable communication between smart devices in Internet of Things (IoT) applications.
- **Examples**:
    - Smart home devices exchanging data without centralized control.
    - Environmental monitoring using sensor networks in remote areas.

5. Temporary Networks for Events

- **Description**: MANETs are ideal for temporary setups like conferences, exhibitions, or outdoor events where infrastructure-based communication is unavailable.
- **Examples**:
    - Real-time collaboration between participants at a conference.
    - Networking among devices at an outdoor concert.

6. Healthcare and Telemedicine

- **Description**: MANETs facilitate real-time communication in remote healthcare settings.
- **Examples**:
    - Remote monitoring of patients in rural or inaccessible areas.
    - Communication between medical devices and healthcare professionals.

7. Collaborative and Peer-to-Peer Communication

- **Description**: MANETs allow devices to share information directly without a centralized server.

- **Examples**:
    - File sharing between devices in a classroom or office.
    - Real-time communication for multiplayer gaming.

8. Underwater and Space Exploration

- **Description**: MANETs support networks in challenging environments like underwater or space, where fixed infrastructure cannot exist.
- **Examples**:
    - Underwater sensor networks for oceanographic studies.
    - Communication between space probes and astronauts.

==========
==========

Challenges of MANETs

While MANETs have numerous applications, they also face significant challenges due to their dynamic and resource-constrained nature:

1. Limited Energy Resources

- **Description**: Nodes in MANETs are often battery-powered, and energy efficiency is critical for the network's longevity.
- **Challenge**:
    - Frequent retransmissions and route discoveries consume significant energy.
    - Protocols must minimize power consumption.

2. Dynamic Topology

- **Description**: Nodes in MANETs are mobile, leading to frequent changes in the network structure.
- **Challenge**:
    - Maintaining stable routes is difficult as nodes move in and out of range.
    - Routing protocols need to adapt quickly to topological changes.

3. Scalability

- **Description**: As the number of nodes increases, network performance may degrade.

- **Challenge**:
    - High node density can cause congestion and interference.
    - Routing protocols must efficiently handle large networks.

4. Security Vulnerabilities

- **Description**: The open wireless medium and decentralized architecture make MANETs prone to attacks.
- **Challenge**:
    - Susceptibility to eavesdropping, spoofing, and denial-of-service (DoS) attacks.
    - Implementing robust security measures without adding excessive overhead.

5. Bandwidth Constraints

- **Description**: MANETs rely on wireless communication, which typically has limited bandwidth.
- **Challenge**:
    - High traffic or large data transfers can lead to congestion.
    - Efficient bandwidth utilization is critical.

6. Routing Overhead

- **Description**: Routing protocols in MANETs require frequent updates due to node mobility.
- **Challenge**:
    - High routing overhead reduces available bandwidth and increases energy consumption.
    - Protocols must balance overhead and routing accuracy.

7. Network Partitioning

- **Description**: Nodes moving out of range can cause the network to split into isolated partitions.
- **Challenge**:
    - Maintaining connectivity between partitions is difficult.
    - Applications requiring continuous communication may face disruptions.

8. Quality of Service (QoS)

- **Description**: Ensuring consistent QoS in MANETs is challenging due to dynamic topology and resource constraints.
- **Challenge**:
    - Applications like real-time video streaming and voice communication require low latency and high reliability.
    - Maintaining QoS is difficult in a constantly changing network.

9. Interference and Signal Degradation

- **Description**: Wireless signals are prone to interference and degradation due to environmental factors.
- **Challenge**:
    - Signal quality may drop in crowded or obstructed environments.
    - Reliable communication in such conditions is a challenge.

10. Coordination in Decentralized Systems

- **Description**: Without a central authority, nodes must coordinate tasks like routing and resource allocation.
- **Challenge**:
    - Ensuring fairness and efficiency in distributed decision-making.
    - Avoiding issues like packet collisions and resource monopolization.

Conclusion

While MANETs offer unparalleled flexibility and applicability in diverse scenarios, their dynamic and resource-constrained nature presents significant challenges. Addressing these challenges requires designing efficient protocols that balance performance, energy efficiency, and security while maintaining scalability and reliability.

==========
==========

Taxonomy of MANET Routing Algorithms

The **taxonomy of MANET (Mobile Ad Hoc Network) routing algorithms** refers to the systematic classification of the various routing protocols used in MANETs. This classification is based on their design principles, working mechanisms, and the challenges they aim to address in dynamic, infrastructure-less networks. Routing algorithms are categorized broadly

into **Topology-Based** and **Position-Based** protocols, with further subcategories depending on how they function and manage routes.

1. Topology-Based Routing Algorithms

2. Position-Based Routing Algorithms

1. Topology-Based Routing Algorithms

Routing in **ad-hoc networks**, such as MANETs (Mobile Ad-hoc Networks), is a challenging task due to the dynamic topology, lack of fixed infrastructure, and limited resources. To manage routing efficiently, various approaches have been developed over time. These approaches are broadly classified into the following three categories:

1. Proactive (Table-Driven) Routing Protocols

In **proactive routing**, each node continuously maintains up-to-date routing information to every other node in the network, even if no communication is required. Each node stores routing tables that are updated periodically, ensuring that routes to all nodes are pre-calculated and available when needed.

Key Features:

- **Routing tables** are maintained at each node.
- Periodic updates are broadcast to keep the tables consistent.
- Routing information is ready for immediate use, leading to low latency when sending data.
- Suitable for networks with low mobility and small node counts.

Advantages:

- Low latency in data transmission as routes are pre-established.
- Route setup time is minimal.

Disadvantages:

- High overhead due to constant routing updates, even when no communication is needed.
- Not scalable for large or highly mobile networks.

Examples of Proactive Routing Protocols:

- **Destination-Sequenced Distance Vector (DSDV)**: Each node maintains a routing table with information about every other node and the shortest path to it.
- **Optimized Link State Routing (OLSR)**: Uses link-state information to calculate routes and reduces overhead by using selected nodes (MPRs, or Multipoint Relays) to broadcast messages.

2. Reactive (On-Demand) Routing Protocols

In **reactive routing**, routes are discovered only when they are needed. When a node wants to send data to a destination, it initiates a route discovery process. The route is then established dynamically and maintained as long as it is needed.

Key Features:

- Routes are created only when required (on-demand).
- No need to maintain routing tables for all nodes at all times.
- Suitable for networks with frequent topology changes and low node density.

Advantages:

- Reduces overhead since routes are not constantly maintained or updated.
- Better suited for larger, more dynamic networks.

Disadvantages:

- Higher latency in data transmission, as routes must be established before data can be sent.
- Route discovery process can introduce delays, especially in high-mobility scenarios.

Examples of Reactive Routing Protocols:

- **Ad-hoc On-Demand Distance Vector (AODV)**: Routes are discovered on demand via a route request (RREQ) and route reply (RREP) mechanism.
- **Dynamic Source Routing (DSR)**: Uses source routing, where the entire route is included in the packet header. Routes are cached and reused if possible.

3. Hybrid Routing Protocols

Hybrid routing combines the advantages of both proactive and reactive approaches. It uses proactive routing within certain zones (usually local or close neighbors) and reactive routing for distant nodes. The goal is to reduce the overhead of proactive routing while minimizing the delay of reactive routing.

Key Features:

- Nodes maintain routes to nearby nodes proactively (within a specific range or zone).
- For distant nodes, routes are discovered on-demand, reducing the need for network-wide updates.
- Suitable for large-scale networks where a balance between overhead and delay is required.

Advantages:

- Balances the trade-off between the overhead of proactive protocols and the latency of reactive protocols.
- Efficient in large networks with diverse node densities and mobility patterns.

Disadvantages:

- Complexity in maintaining different routing strategies for local and distant nodes.
- More complicated to implement compared to purely proactive or reactive protocols.

Examples of Hybrid Routing Protocols:

- **Zone Routing Protocol (ZRP)**: Divides the network into zones. Proactive routing is used within a zone, while reactive routing is used for nodes outside the zone.
- **Hybrid Ad-hoc Routing Protocol (HARP)**: Combines the efficiency of proactive routing for frequently used routes and the flexibility of reactive routing for other routes.

Summary of Routing Approaches:

- **Proactive routing** ensures immediate route availability at the cost of higher overhead due to constant updates.
- **Reactive routing** reduces overhead but introduces delays as routes must be discovered before data transmission.
- **Hybrid routing** balances the strengths and weaknesses of both approaches, using proactive routing for nearby nodes and reactive routing for distant ones.

These approaches aim to provide efficient routing solutions tailored to the dynamic and resource-constrained nature of ad-hoc networks.

==========
==========

DSDV

Proactive Routing Protocol: DSDV (Destination-Sequenced Distance Vector Protocol)

Introduction:

- DSDV is a table-driven proactive routing protocol designed to provide loop-free routing using sequence numbers.
- Nodes in the network continuously maintain up-to-date routing tables, ensuring that routes to all destinations are readily available.

Working Mechanism:

1. **Routing Table Management:**
    - Each node maintains a table with the following:
        - Destination address.
        - Next hop to the destination.
        - Number of hops required.
        - Sequence numbers indicating the freshness of the route.
2. **Periodic Updates:**
    - Nodes broadcast their routing tables periodically to their neighbors.
    - Updates can be:
        - **Full dumps**: The entire table.
        - **Incremental updates**: Only changes since the last update.
3. **Sequence Numbers:**
    - Assigned by the destination, sequence numbers help identify the most recent route and prevent loops.

Example:

- Consider a MANET with nodes A, B, and C:
    - Node A wants to send data to node C.
    - The routing table of A might have:
        - Destination: C, Next Hop: B, Hops: 2, Sequence: 5.
    - If C moves, it increments the sequence number (e.g., to 6) and broadcasts the new route, ensuring updates across the network.

Advantages:

- Immediate route availability minimizes delays.
- Ensures loop-free routing using sequence numbers.

Disadvantages:

- High control overhead due to frequent updates.
- Inefficient in highly dynamic networks.

==========

Dynamic Source Routing Protocol (DSR):

1. **Route Discovery:**
    - Initiated when a source node (S) needs a route to a destination (D).
    - S broadcasts a Route Request (RREQ), which is forwarded by intermediate nodes, recording the path.
2. **Route Reply:**
    - When D receives RREQ, it sends a Route Reply (RREP) back to S along the reverse path.
3. **Source Routing:**
    - The entire path to the destination is included in packet headers, reducing intermediate node dependency.

Example:

- If node A wants to communicate with E, it broadcasts RREQ:
    - RREQ: A → B → C → D → E.
    - RREP: E → D → C → B → A.
- Future packets from A to E use this cached route.

Advantages:

- Efficient in small, low-traffic networks.
- Reduces memory overhead at intermediate nodes.

Disadvantages:

- High delay during route discovery.
- Packet headers grow with path length.

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

1. **Route Discovery:**
    - Similar to DSR, AODV uses RREQ and RREP messages.
    - Intermediate nodes maintain routing tables, recording only the next hop.
2. **Sequence Numbers:**
    - Ensure fresh and loop-free routes.
3. **Route Maintenance:**
    - Nodes send Route Error (RERR) messages when a link breaks.

Example:

- Node A wants to send data to D:
    - A sends RREQ: A → B → C → D.
    - D responds with RREP: D → C → B → A.
    - Only the next hop is stored, reducing overhead.

Advantages:

- Reduces memory usage compared to DSR.
- Adaptable to topology changes.

Disadvantages:

- Route discovery latency.
- Frequent broadcasting in large networks

==========
==========

Hybrid Routing Protocol: ZRP (Zone Routing Protocol)

Introduction:

ZRP combines proactive and reactive strategies to balance the trade-offs between routing overhead and latency. The network is divided into **zones**, defined by a fixed radius.

Working Mechanism:

1. **Intra-Zone Routing:**
    - Proactive routing is used within a zone.
    - Nodes maintain routing tables for all nodes in their zone.
2. **Inter-Zone Routing:**
    - Reactive routing is used between zones.
    - Border nodes handle queries for destinations outside the zone.

Example:

- Consider a network with a zone radius of 2 hops:
    - Node A communicates with node F (4 hops away).
    - A's intra-zone routing identifies border node C.
    - C initiates reactive discovery to locate F.

Advantages:

- Reduces control overhead for distant routes.
- Low latency for intra-zone communication.

Disadvantages:

- Performance depends on zone radius.
- Complex zone maintenance in dynamic networks.

Taxonomy of Routing Protocols

Routing protocols can be classified based on criteria like:

- **Routing Information:** Proactive, reactive, hybrid.
- **Topology:** Flat, hierarchical.
- **Route Metrics:** Hop count, energy, delay.

==========
==========

Forwarding Strategies in MANETs

Forwarding strategies in Mobile Ad Hoc Networks (MANETs) define how data packets are transmitted from a source to a destination. Unlike traditional networks with static infrastructures, MANETs require efficient forwarding mechanisms due to dynamic topologies, node mobility, and limited resources. Below are explanations of some key forwarding strategies:

---

1. Greedy Packet Forwarding

Greedy forwarding is a position-based routing strategy where packets are forwarded to the neighbor closest to the destination.

Working Mechanism:

- Each node is aware of its own position, the positions of its neighbors, and the position of the destination using techniques like GPS or location services.
- When forwarding a packet:

1. The current node calculates the distance of its neighbors to the destination.
2. The neighbor closest to the destination is selected as the next hop.
3. This process repeats until the packet reaches the destination.

Example:

- Consider a network with nodes A, B, C, and D, where A is the source and D is the destination.
    - Node A forwards the packet to B because B is geographically closer to D.
    - Node B forwards it to C, and finally, C delivers it to D.

Advantages:

- Simple and efficient in dense networks.
- Reduces routing overhead as it does not require global topology knowledge.

Disadvantages:

- **Local Maxima Problem:** If a node has no neighbor closer to the destination, the packet may get "stuck."
- Performance decreases in sparse networks.