Lecture 6: Ad hoc and Mesh Networks

6.1. Ad hoc Network Concepts and Challenges
6.1.1. Concepts
6.1.2. Challenges

6.2. Ad hoc Routing Protocols: AODV, DSR, and OLSR
6.2.1. AODV (Ad Hoc On-Demand Distance Vector)
6.2.2. DSR (Dynamic Source Routing)
6.2.3. OLSR (Optimized Link State Routing)

6.3. Mesh Network Architectures and Protocols
6.3.1 Mesh Network Architectures
6.3.2. Mesh Network Protocols
6.3.3. Challenges and Considerations

6.4. Self-Organization and Network Management in Ad Hoc and Mesh Networks
6.4.1. Self-Organization in Ad Hoc and Mesh Networks
6.4.2. Network Management in Ad Hoc and Mesh Networks
6.4.3. Challenges and Considerations

6.1. Ad hoc Network Concepts and Challenges

- ***Ad hoc networks*** are decentralized wireless networks where nodes communicate directly with each other without relying on a fixed infrastructure like access points or base stations.

- These networks are highly dynamic and self-configuring, making them suitable for scenarios where a pre-established network infrastructure is unavailable or impractical.

6.1.1. Concepts

1. ***Decentralization***: Ad hoc networks are characterized by a lack of centralized control. Nodes act as both users and routers, contributing to network connectivity.

2. ***Node Mobility***: Nodes in ad hoc networks can be stationary or mobile. Mobility can disrupt network topology, making routing and connectivity management challenging.

3. ***Dynamic Topology***: The network topology changes frequently due to node mobility, node failures, or energy depletion. This dynamic nature requires adaptive routing and self-configuration mechanisms.

4. ***Spontaneous Formation***: Ad hoc networks can be established spontaneously, such as during emergency situations or military operations. Nodes join the network as needed without prior planning.

5. ***Resource Constraints***: Nodes in ad hoc networks often have limited resources, including battery power, processing capacity, and memory. Efficient resource management is essential.

6. ***Scalability***: Ad hoc networks can vary in size from small-scale, ad hoc group communications to large-scale deployments covering vast areas. Scalability is a critical consideration.

6.1.2. Challenges

1. ***Routing***: Finding efficient routes for data transmission in a dynamic and potentially disrupted topology is a fundamental challenge. Reactive (on-demand) and proactive (table-driven) routing protocols are used to address this challenge.

2. ***Network Management***: Self-organizing and self-healing capabilities are necessary for managing network resources, adapting to topology changes, and ensuring network stability.

3. ***Node Mobility***: Coping with node mobility requires adaptive routing protocols and mechanisms to handle link failures due to nodes moving out of range.

4. ***Security***: Ad hoc networks are susceptible to various security threats, including eavesdropping, data tampering, and malicious node attacks. Implementing robust security mechanisms is essential.

5. ***Quality of Service (QoS)***: Ensuring QoS in ad hoc networks, particularly for real-time applications like voice and video, is challenging due to dynamic conditions and limited resources.

6. ***Scalability***: Ad hoc networks must be designed to scale effectively to accommodate varying numbers of nodes and traffic loads.

7. ***Energy Efficiency***: Nodes in ad hoc networks are often powered by batteries, making energy-efficient communication and routing critical to prolong network operation.

8. ***Interoperability***: Ad hoc networks may need to interoperate with other network types, such as infrastructure-based networks or the internet, posing interoperability challenges.

9. ***Resource Discovery***: Nodes must discover and utilize available network resources efficiently, considering limited bandwidth and energy constraints.

10. ***Privacy***: Protecting user privacy in ad hoc networks is a concern, especially when nodes can communicate directly with each other.

11. ***Routing Overhead***: Minimizing the control message overhead required for route discovery and maintenance is essential to maximize available bandwidth.

6.2. Ad hoc Routing Protocols: AODV, DSR, and OLSR

- ***Ad hoc routing protocols*** are essential for establishing and maintaining communication paths in dynamic and self-configuring wireless networks like ad hoc networks.

- Three prominent protocols in this category are AODV (Ad Hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and OLSR (Optimized Link State Routing).

- Each of these protocols employs distinct strategies for routing data in ad hoc networks:

6.2.1. AODV (Ad Hoc On-Demand Distance Vector)

Key Features:

- On-Demand Routing: AODV is an on-demand, reactive routing protocol. It creates routes only when needed, reducing control message overhead compared to proactive protocols like OLSR.

- Route Discovery: When a node wants to send data to a destination for which it has no route, it initiates a route discovery process. The source broadcasts a Route Request (RREQ) packet. Intermediate nodes forward the RREQ until it reaches the destination or a node with a fresh route to the destination.

- Route Maintenance: AODV uses sequence numbers to prevent routing loops and ensure route freshness. If a link or route becomes invalid (e.g., due to node mobility or link failure), the source node can initiate route discovery to find an alternative path.

Pros:

- Low control message overhead.
- Suitable for networks with variable traffic patterns.
- Efficient for networks with infrequent communication needs.

Cons:

- Delay in route establishment when routes are not pre-existing.
- May not perform optimally in highly mobile networks.

6.2.2. DSR (Dynamic Source Routing)

Key Features:

- ***Source Routing***: DSR is a source routing protocol. In DSR, the source node includes the complete route in the packet header. Intermediate nodes use this header information to forward the packet to the next hop.

- ***Route Caching***: DSR nodes cache discovered routes. Cached routes can be reused for subsequent data packets, reducing latency and control overhead.

- ***Route Maintenance***: DSR employs route maintenance mechanisms. If a node detects that a route is no longer valid (e.g., due to link failure or node mobility), it can initiate route discovery to find an alternative path.

Pros:

- Low control message overhead within the network.
- Supports multiple routes to a destination.
- Efficient for networks with a moderate number of nodes.

Cons:

- Large routing overhead in the source packet header, which can increase packet size.
- Requires more memory for route caching.

6.2.3. OLSR (Optimized Link State Routing)

Key Features:

- ***Link State Protocol***: OLSR is a proactive, table-driven routing protocol. It maintains a table of link states, allowing nodes to compute routes based on up-to-date information.

- ***Multipoint Relays (MPRs)***: OLSR introduces the concept of Multipoint Relays (MPRs) to optimize flooding in the network. MPR nodes are selected to forward control messages, reducing control message overhead.

- ***Low Control Traffic***: OLSR minimizes control message exchange, making it suitable for networks with relatively stable topologies.

Pros:

- Fast route establishment since routes are pre-computed.
- Low control message overhead within the network.
- Efficient for networks with stable topologies.

Cons:

- May not adapt well to highly dynamic networks with frequent topology changes.
- Increased memory requirements for storing routing tables.

6.3. Mesh Network Architectures and Protocols

- ***Mesh networks*** are decentralized wireless networks characterized by their interconnected, self-routing nodes.

- They offer robustness, redundancy, and flexibility, making them suitable for a wide range of applications, from home automation to large-scale industrial deployments.

6.3.1 Mesh Network Architectures

1. ***Full Mesh Architecture***: In a full mesh, every node is connected to every other node. This architecture ensures redundancy and high fault tolerance but can be impractical in large networks due to the high number of connections required.

2. ***Partial Mesh Architecture***: In a partial mesh, nodes are selectively interconnected. This reduces the number of connections while maintaining redundancy and fault tolerance. Nodes are strategically placed to ensure connectivity.

3. ***Ad Hoc Mesh Architecture***: Ad hoc mesh networks are dynamic and self-organizing. Nodes communicate with nearby nodes to establish and maintain connections. This architecture is common in mobile ad hoc networks (MANETs).

4. ***Infrastructure Mesh Architecture***: Infrastructure mesh networks include access points or gateways that provide connectivity to the wider internet or other networks. These gateways are strategically placed, and nodes communicate through them.

6.3.2. Mesh Network Protocols

1. ***802.11s:*** This IEEE standard defines a mesh networking protocol for wireless LANs. It enables Wi-Fi devices to create self-configuring and self-healing mesh networks. 802.11s is often used in home automation and community networks.

2. ***B.A.T.M.A.N. (Better Approach To Mobile Ad-hoc Networking):*** B.A.T.M.A.N. is a proactive, table-driven routing protocol used in ad hoc mesh networks. It employs a proactive approach, meaning that it constantly updates routing tables to maintain connectivity. It's popular in community networks and open-source projects.

3. ***OLSR (Optimized Link State Routing):*** As mentioned earlier, OLSR is a proactive routing protocol that optimizes link state routing for mesh networks. It's designed for large-scale deployments with stable topologies.

4. ***MANET Routing Protocols:*** Mesh networks often employ mobile ad hoc network (MANET) routing protocols like AODV, DSR, and TORA (Temporally Ordered Routing Algorithm) to establish and maintain routes between nodes. These protocols are suitable for dynamic and mobile mesh environments.

5. ***Zigbee:*** Zigbee is a low-power, low-data-rate wireless mesh networking protocol commonly used in home automation and industrial applications. It's designed for devices with limited resources and can form self-healing mesh networks.

6. ***Thread:*** Thread is an IPv6-based mesh networking protocol developed for the Internet of Things (IoT). It's designed to provide secure and reliable communication in smart home and industrial applications.

6.3.3. Challenges and Considerations

- ***Routing***: Efficient routing in mesh networks is a challenge due to the dynamic nature of wireless links and node mobility. Proactive and reactive routing protocols are used to address this challenge.

- ***Scalability***: Designing scalable mesh networks requires careful consideration of how nodes are organized and how routing scales with network size.

- ***Interference***: Interference from neighboring nodes can affect signal quality and throughput. Mesh networks must employ interference mitigation techniques.

- ***Security***: Securing mesh networks is crucial, especially when used in critical applications. Encryption, authentication, and intrusion detection mechanisms are essential.

- ***Power Management***: Power efficiency is critical in battery-operated devices. Mesh networks often implement low-power modes and sleep schedules to extend device battery life.

- ***Topology Control***: Managing the topology of a mesh network is essential to ensure efficient routing and minimize interference. Some protocols use centralized controllers for topology control.

6.4. Self-Organization and Network Management in Ad Hoc and Mesh Networks

- ***Ad hoc and mesh networks*** are characterized by their self-organizing nature, where nodes collaborate to establish and maintain network connectivity without centralized control.

- This self-organization is essential for their dynamic and decentralized operation.

6.4.1. Self-Organization in Ad Hoc and Mesh Networks

1. ***Decentralization***: Ad hoc and mesh networks do not rely on a central controller or infrastructure. Nodes in these networks are equal, and each node can act as a router, collaboratively forwarding data packets.

2. ***Dynamic Topology***: These networks have dynamic topologies where nodes can join or leave the network at any time. Nodes must adapt to topology changes quickly, making self-organization critical.

3. ***Autonomous Operation***: Nodes make autonomous decisions regarding routing, forwarding, and network management. They use distributed algorithms to determine routes and configure themselves.

4. ***Neighbor Discovery***: Nodes perform neighbor discovery to identify neighboring nodes within their communication range. This information is crucial for routing decisions and network maintenance.

6.4.2. Network Management in Ad Hoc and Mesh Networks

1. ***Routing Protocols***: Network management in these networks involves the selection and configuration of routing protocols. Depending on the network's requirements and characteristics, protocols like AODV, DSR, OLSR, or proprietary solutions may be chosen.

2. ***Topology Control***: Managing the network's topology is essential to optimize routing and reduce interference. Some protocols employ mechanisms to control the transmission power of nodes or select specific nodes as leaders for topology management.

3. ***Quality of Service (QoS):*** Ensuring QoS in ad hoc and mesh networks can be challenging due to their dynamic nature. Network management may involve mechanisms for prioritizing traffic and managing bandwidth.

4. ***Security***: Security management is critical, especially in open or public mesh networks. It includes mechanisms for authentication, encryption, intrusion detection, and secure key management.

5. ***Resource Management***: Ad hoc and mesh networks often operate under resource constraints, such as limited battery power in mobile devices. Managing resources efficiently is essential for network longevity. This may involve power management and resource-aware routing.

6. ***Scalability***: As networks grow, network management should support scalability. This includes addressing issues related to routing scalability, control message overhead, and node management.

6.4.3. Challenges and Considerations

1. ***Dynamic Nature***: The dynamic topology of these networks requires adaptive and self-healing routing algorithms. Network management must handle frequent topology changes effectively.

2. ***Resource Constraints***: Many nodes in these networks are resource-constrained devices, which adds complexity to network management. Energy-efficient operation and resource-awareness are essential.

3. ***Interference Mitigation***: In wireless networks, interference from neighboring nodes can impact network performance. Effective network management may include interference mitigation techniques.

4. ***Security***: Ensuring the security of self-organizing networks is challenging. Network management should address vulnerabilities and implement security mechanisms.

5. ***Quality of Service***: Meeting QoS requirements in dynamic networks is difficult. Network management should consider traffic prioritization and adaptive QoS mechanisms.

6. ***Standardization***: In some cases, proprietary solutions coexist with standardized protocols. Network management should address interoperability and standard compliance.

7. ***Deployment Scenarios***: The specific application and deployment scenario greatly influence network management requirements. Different applications may prioritize different aspects of network management.