Mobile and Adhoc Computing Ques. Bank Solution

- Aditya Dhiman

Unit 1

Q1. What do you understand by Adhoc Network?
An Adhoc Network is a decentralized wireless network where devices communicate directly without the need for pre-existing infrastructure like routers or access points. Each device acts as both a client and a router to forward data to other devices in the network.

Q2. Define Wireless Network? Explain its properties.
A Wireless Network enables communication between devices without using physical cables, typically using radio waves. Properties of wireless networks include mobility, flexibility, scalability, and the ability to connect multiple devices without physical connections.

Q3. What is Cellular Network?
A Cellular Network is a type of wireless communication network divided into small geographic areas called cells, each served by a base station. It is used in mobile phones to allow communication while moving between different locations within the network.

Q4. Explain which switching technology is governed by Adhoc and Cellular Network?
Adhoc Networks primarily use **packet switching**, where data is broken into packets and routed dynamically. Cellular Networks can use both **circuit switching** (in voice calls) and **packet switching** (in data services).

Q5. Explain what do you understand by handoff?
Handoff is the process of transferring an active call or data session from one base station or cell tower to another as a user moves through the coverage area of a mobile network, ensuring uninterrupted service.

Q6. Describe the applications of Adhoc Network.
Applications of Adhoc Networks include military operations (battlefield communication),

emergency disaster response, sensor networks, vehicular networks, and personal area networks like Bluetooth connections.

Q7. Explain the Advantages and Disadvantages of Adhoc Network.
Advantages:

- Flexibility in establishing the network without infrastructure.
- Cost-effective and scalable.
  Disadvantages:
- Limited bandwidth and high power consumption.
- Unstable due to dynamic topology and lack of centralized management.

Q8. Explain the issues related to the MAC layer.
Issues related to the MAC (Medium Access Control) layer in wireless networks include collision avoidance, hidden terminal problems, and power control challenges. These issues can impact network efficiency and performance.

Q9. List some of the characteristics of wireless channels.
Characteristics of wireless channels include:

- Time-varying nature due to mobility.
- Multipath propagation causing signal fading.
- Limited bandwidth and high error rates compared to wired channels.

Q10. Explain Packet Switching in detail.
Packet Switching is a communication method where data is divided into small packets and transmitted over a network. Each packet may take a different path to the destination, where the packets are reassembled. It is efficient for handling bursty data and supports multiple connections simultaneously.

Q11. Explain Circuit Switching in detail.
Circuit Switching involves establishing a dedicated communication path between two nodes

for the duration of a session. It is used in traditional telephony, providing a constant and guaranteed data rate but is less efficient than packet switching for bursty data.

Q12. What are the shortcomings of Wireless Adhoc Network?
Shortcomings of Wireless Adhoc Networks include limited scalability, high power consumption, security vulnerabilities, and unpredictable performance due to the dynamic topology of the network.

Q13. What do you understand by QoS in Adhoc Network?
QoS (Quality of Service) in an Adhoc Network refers to the ability to provide predictable and guaranteed performance metrics like bandwidth, delay, jitter, and packet loss, which are crucial for real-time applications.

Q14. Differentiate between Proactive, Reactive, and Hybrid routing.

- **Proactive Routing:** Constantly maintains updated routes to all nodes, e.g., DSDV.
- **Reactive Routing:** Routes are only created when needed, e.g., AODV.
- **Hybrid Routing:** Combines proactive and reactive approaches, e.g., ZRP.

Q15. What are the benefits in terms of infrastructure in Adhoc Network?
Adhoc Networks eliminate the need for centralized infrastructure, making them cost-effective and easy to deploy in remote areas or situations where traditional infrastructure is unavailable or unreliable.

Q16. What do you understand by Routing in Mobile Adhoc Network?
Routing in a Mobile Adhoc Network (MANET) refers to the process of finding and maintaining paths between nodes that may frequently change their positions due to the mobile nature of the network.

Q17. Why is it called an Adhoc Network?
It is called an Adhoc Network because it is formed on an as-needed basis, without any fixed infrastructure or central management, allowing devices to communicate directly.

Q18. Explain Hybrid Routing in detail.
Hybrid Routing in Adhoc Networks combines the advantages of both proactive and reactive routing strategies. It uses proactive routing for nearby nodes to reduce latency and reactive routing for distant nodes to reduce overhead. An example of a hybrid routing protocol is the Zone Routing Protocol (ZRP).

Q19. Explain how Sensitivity affects QoS in Adhoc Network.
Sensitivity in an Adhoc Network affects QoS by influencing how well the network can detect and react to changes in signal strength and interference. Higher sensitivity improves detection but may increase false positives, while lower sensitivity reduces the ability to detect weak signals.

Q20. Explain in detail how the density of nodes and hop count affect QoS in Adhoc Networks.
The density of nodes and hop count directly impact the QoS in Adhoc Networks. A higher node density increases the chances of interference and collisions but improves route availability. A higher hop count can lead to increased delay and packet loss due to longer paths and more intermediate nodes, negatively affecting the network's performance.

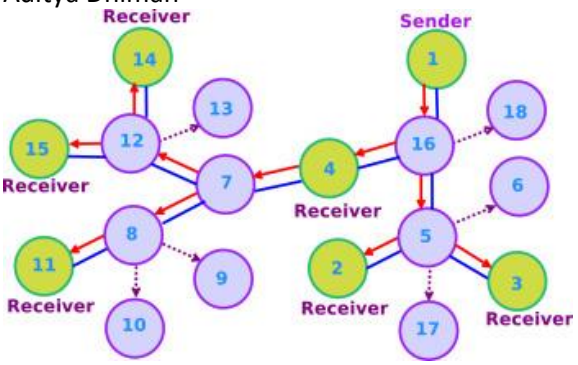
Level B

Q21. Explain with examples and diagrams where-ever required Tree-based and Mesh-based Protocols in detail?

Tree-Based Protocols:
Tree-based protocols in wireless networks organize nodes into a hierarchical structure resembling a tree, with a root node acting as the central point for all communication. Routing decisions are made based on this tree structure to ensure that packets are efficiently routed.

- **Example:** The multicast routing protocol **MAODV (Multicast Ad-hoc On-Demand Distance Vector)** uses a tree structure for multicast routing. The root node manages routing paths, ensuring data flows from the sender to receivers using branches.

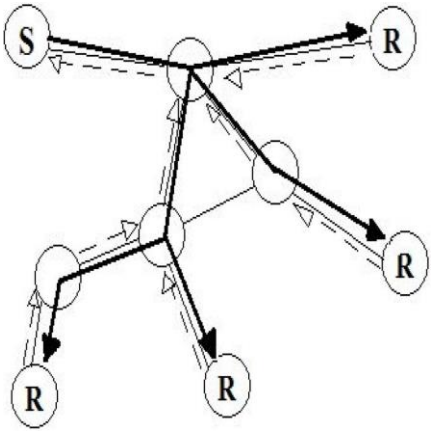
Diagram:



Mesh-Based Protocols:
Mesh-based protocols do not rely on a centralized structure but instead create multiple paths between nodes to ensure redundancy and fault tolerance. These protocols are more resilient to failures as multiple routes exist between any pair of nodes.

- **Example: ODMRP (On-Demand Multicast Routing Protocol)** is a mesh-based protocol where each node establishes multiple routes to ensure data delivery even if some nodes fail.

Diagram:



Q22. What is Multicast with Quality of Service Provision?

Multicast with QoS Provision:
Multicasting refers to the process of sending data to a group of destination nodes simultaneously over a network. **Multicast with Quality of Service (QoS)** ensures that not only is data efficiently delivered to multiple destinations, but it also meets specific performance metrics like bandwidth, latency, and jitter.

- **Example:** In a video conferencing scenario, multicast with QoS ensures that video streams reach all participants simultaneously with minimal delay or packet loss.
- **QoS Parameters:** To ensure QoS, parameters such as **bandwidth** (ensuring adequate bandwidth for the session), **latency** (low delays in transmission), and **jitter** (minimal variation in packet arrival time) are monitored and maintained.

Q23. Write short notes on Reactive Routing, Coverage, Signal Strength, and Bandwidth.

Reactive Routing:
Reactive routing protocols create routes only when needed. Unlike proactive routing, it doesn't maintain routes to all nodes in advance, saving resources but increasing latency for route discovery.

- **Example: AODV (Ad-hoc On-demand Distance Vector)** protocol.

Coverage:
Coverage in wireless networks refers to the geographic area within which a node can communicate with others. The size and quality of the coverage depend on factors such as transmission power and environmental conditions.

Signal Strength:
Signal strength refers to the power level received by a node from another device. Stronger signals result in better communication quality, while weaker signals may lead to higher error rates or disconnections.

Bandwidth:
Bandwidth is the data-carrying capacity of a communication channel. In Adhoc networks, available bandwidth is shared among nodes, and ensuring enough bandwidth is crucial for applications with high data requirements like video streaming.

Q24. What are the different parameters that decide the Quality of Service (QoS) of Adhoc Network?

The QoS of an Adhoc network is determined by several key parameters:

1. **Throughput:** The total data successfully delivered over the network. Higher throughput implies better network performance.
2. **Latency:** The time delay in data transmission. Low latency is essential for real-time applications.

3. **Jitter:** The variation in packet arrival times. Consistent packet delivery ensures smoother performance for audio/video applications.
4. **Packet Loss:** The percentage of packets lost during transmission. Reducing packet loss is critical for data integrity.
5. **Bandwidth:** Adequate bandwidth ensures the network can handle the required data load without congestion.
6. **Power Consumption:** In mobile Adhoc networks, power-efficient routing and transmission are crucial due to the battery constraints of mobile nodes.

Q25. Explain about the Security of MANET in point form.

- **Decentralization:** MANETs lack a centralized infrastructure, making security more complex.
- **Authentication:** Ensuring that nodes are who they claim to be is challenging without a trusted central authority.
- **Encryption:** Data encryption helps to protect the confidentiality and integrity of communication.
- **Intrusion Detection Systems (IDS):** MANETs can deploy IDS to detect abnormal behaviors like routing attacks.
- **Routing Attacks:** MANETs are vulnerable to various routing attacks like **black hole attacks**, where malicious nodes discard data packets.
- **Key Management:** Securely distributing and managing cryptographic keys in a decentralized environment is difficult.
- **Physical Vulnerability:** Nodes in MANETs are mobile and can be physically captured, leading to compromised security.

Q26. Explain in detail about different types of Routing Algorithm.

Proactive Routing Algorithms:
These algorithms maintain up-to-date routing information by periodically exchanging routing tables with all nodes. They provide immediate route availability but suffer from high control overhead.

- **Example: DSDV (Destination-Sequenced Distance-Vector)** routing.

Reactive Routing Algorithms:
These algorithms create routes only when needed, saving bandwidth but introducing delay during route discovery.

- **Example: AODV (Ad-hoc On-demand Distance Vector)**.

Hybrid Routing Algorithms:
Hybrid routing algorithms combine the features of both proactive and reactive approaches. They use proactive routing for nearby nodes and reactive routing for distant nodes, balancing efficiency and overhead.

- **Example: ZRP (Zone Routing Protocol)**.

Q27. What are fixed infrastructure networks? What are the problems with fixed infrastructure networks? Explain the Architecture of MANET.

Fixed Infrastructure Networks:
Fixed infrastructure networks rely on pre-established infrastructure such as base stations, routers, and switches to manage communication between devices.

Problems with Fixed Infrastructure Networks:

- **Limited Flexibility:** Cannot handle rapid changes in topology or mobility of nodes.
- **High Cost:** Requires expensive infrastructure and maintenance.
- **Failure Points:** A failure in the infrastructure can disrupt the entire network.

Architecture of MANET:
MANETs are infrastructure-less networks where nodes are free to move. Each node acts as both a host and a router, forwarding data for others. Nodes communicate directly with each other without the need for central infrastructure, making MANETs flexible and scalable but also challenging in terms of routing, security, and QoS.

Q28. What do you understand by Exposure and Event in QoS Provision? Explain with the help of a diagram and example.

Exposure:
In the context of QoS, exposure refers to how much information a node in an Adhoc network has about the network's state (such as node positions, traffic, and signal quality). High exposure helps in better decision-making regarding routing and resource allocation.

Event in QoS Provision:
An event refers to a change in the network that affects QoS, such as a node moving out of range or a sudden increase in traffic load. Events can degrade QoS unless the network adapts to handle them.

Example:
In a video streaming scenario, exposure would involve knowing the signal strength and available bandwidth, while an event might be a node moving out of range, causing a drop in video quality.

Q29. What do you understand by Proactive Routing Protocol? Explain in detail with examples.

Proactive Routing Protocols:
These protocols maintain fresh lists of routes by periodically distributing routing tables across the network, ensuring that routes are available immediately when needed. However, the constant exchange of routing information can lead to high control overhead.

- **Example: OLSR (Optimized Link State Routing Protocol)** periodically updates link-state information, allowing nodes to immediately determine the shortest path to any destination in the network.

Proactive protocols work well in networks with stable topologies but may struggle in highly dynamic environments due to their high overhead.

Q30. MAC Layer has multiple issues related to Routing. Explain them in detail.

Hidden Terminal Problem:
When two nodes are out of range of each other but can communicate with a common node, their simultaneous transmissions may collide, causing interference and data loss.

Exposed Terminal Problem:
A node refrains from transmitting even though its transmission wouldn't cause a collision, resulting in underutilization of the available bandwidth.

Channel Allocation:
In Adhoc networks, dynamic and efficient allocation of the shared communication channel is crucial to prevent congestion and ensure fair access for all nodes.

Interference and Collision:
Multiple nodes transmitting simultaneously can interfere with each other, leading to packet collisions and reduced throughput.

These MAC layer issues can degrade network performance, especially in dynamic environments like MANETs, where nodes frequently join or leave the network.

Level C

Q31. Compare Reactive and Hybrid Routing Protocols. Use diagrams and examples where required

Reactive Routing Protocols:
Reactive protocols, also known as **on-demand protocols**, create routes only when needed. These protocols do not maintain an up-to-date list of routes, which saves resources but introduces latency during route discovery.

- **Example: AODV (Ad-hoc On-demand Distance Vector)** routing protocol, where routes are created when a node requests communication with another.

Advantages of Reactive Protocols:

- No need for constant route maintenance.
- Lower overhead, making it ideal for dynamic networks.

Disadvantages:

- Higher latency due to route discovery.
- Frequent route requests in large networks can lead to congestion.

Hybrid Routing Protocols:
Hybrid routing protocols combine the benefits of both proactive and reactive routing. Nodes within a certain distance (zone) use proactive routing, while distant nodes rely on reactive routing.

- **Example: ZRP (Zone Routing Protocol)**, where nearby nodes proactively maintain routes, and distant nodes use reactive discovery.

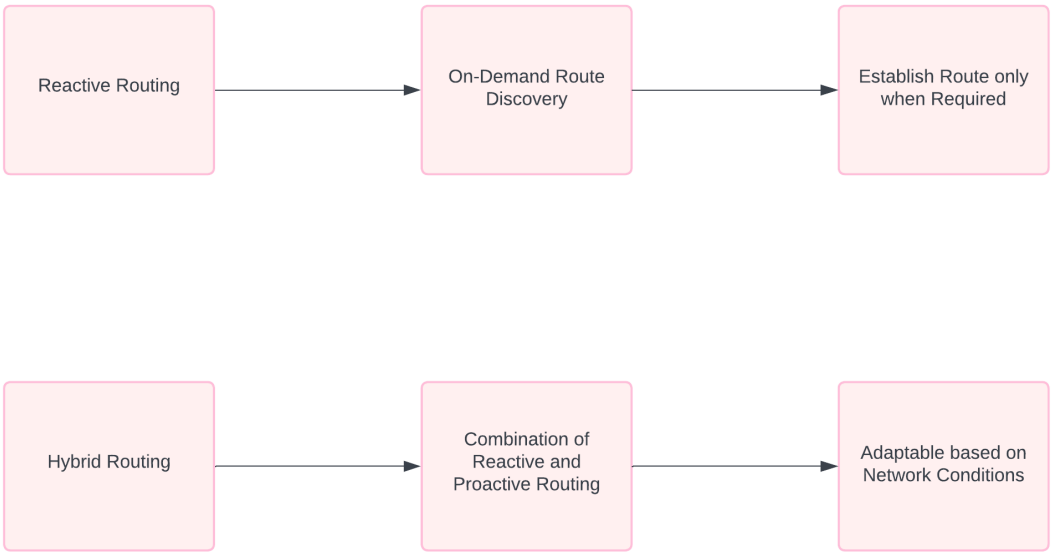
Advantages of Hybrid Protocols:

- Efficient use of bandwidth for nearby nodes.
- Lower latency for local communication.

Disadvantages:

- More complex than pure reactive or proactive protocols.

Diagram:



Q32. Explain in detail with example about Link State Algorithm and Distance Vector Algorithm

Link State Algorithm:
The Link State algorithm (LSA) maintains a complete map of the network. Each node independently calculates the shortest path to every other node by flooding the network with its link state information.

- **Example: OSPF (Open Shortest Path First)** is a protocol that uses LSA. Nodes broadcast information about their neighbors, and each node builds a full map of the network to find the best route.

Steps in Link State Algorithm:

1. Each node learns about its neighbors.
2. Nodes broadcast their link-state information to the entire network.
3. Every node builds a complete map of the network.
4. Nodes compute the shortest path using algorithms like Dijkstra's algorithm.

Distance Vector Algorithm:
The Distance Vector algorithm works by having each node share its distance to all destinations with its immediate neighbors. Based on this, nodes build routing tables.

- **Example: RIP (Routing Information Protocol)** uses the Distance Vector algorithm.

Steps in Distance Vector Algorithm:

1. Each node maintains a routing table with distances to all nodes.
2. Nodes exchange their routing tables with neighbors.
3. Nodes update their tables based on neighbors' information using algorithms like Bellman-Ford.

Comparison:
While LSA provides a more accurate and up-to-date picture of the network, it is more resource-intensive. Distance Vector algorithms are simpler but can suffer from issues like routing loops.

Q33. Explain the Characteristics of Mobile Adhoc Network (MANET)? Also explain its Pros and Cons? What are the improvements in MANET?

Characteristics of MANET:

1. **Decentralized Architecture:** MANETs operate without a centralized infrastructure, making them flexible.
2. **Dynamic Topology:** Nodes can freely move, join, or leave the network, causing constant topology changes.
3. **Multi-Hop Routing:** Communication occurs via multiple nodes since direct communication between distant nodes is often impossible.
4. **Self-Organizing:** Nodes manage themselves and establish connections dynamically.
5. **Limited Resources:** MANETs often operate with constraints like low bandwidth, limited battery life, and processing power.

Pros of MANET:

- **Flexibility:** Can be deployed in areas without infrastructure.
- **Cost-Effective:** No need for base stations or fixed infrastructure.
- **Scalability:** Can easily expand or contract based on the number of nodes.

Cons of MANET:

- **Security Issues:** Lack of infrastructure makes it difficult to manage security.
- **Unreliable Communication:** Node mobility and interference can lead to packet loss and disconnection.
- **Limited Bandwidth and Power:** The decentralized nature places strain on resources like power and bandwidth.

Improvements in MANET:

- **Security Enhancements:** Techniques like encryption and intrusion detection systems (IDS) are improving network security.
- **QoS Improvements:** Advances in routing protocols are helping to maintain QoS despite the dynamic topology.
- **Energy-Efficient Protocols:** New algorithms aim to reduce energy consumption, extending the lifespan of nodes.

Q34. Differentiate between Mobile Adhoc Network (MANET) and Wireless Sensor Network (WSN) in tabular form considering its features.

Feature	MANET	Wireless Sensor Network (WSN)
Purpose	General-purpose communication	Specific-purpose data sensing and gathering
Node Type	General nodes (e.g., smartphones)	Sensor nodes (limited in power, memory)
Topology	Highly dynamic	Typically static or semi-static
Communication	Peer-to-peer	Multi-hop, often centralized for data collection
Power Supply	Can vary, but often battery-operated	Typically energy-constrained, powered by batteries
Data Focus	General data communication	Sensing environmental or physical data

Feature	MANET	Wireless Sensor Network (WSN)
Routing	Focuses on efficient pathfinding	Focuses on energy efficiency and data aggregation
Security Concerns	Vulnerable due to lack of central control	Often secure due to physical node distribution
Application	Emergency services, military	Environmental monitoring, health systems

---

Q35. What is Multicasting? Define Computer Network and explain its two components.

Multicasting:
Multicasting is a method of sending data to a group of nodes simultaneously rather than sending data to each node individually. This is efficient for applications like video conferencing or streaming, where the same data is delivered to multiple users at the same time.

Computer Network:
A computer network is a system that connects computers and other devices to exchange data. It allows sharing of resources, such as files and printers, and communication through services like email and messaging.

Components of a Computer Network:

1. **Nodes (End Devices):** These are devices like computers, smartphones, and printers that are part of the network. Nodes generate, receive, and process data.
2. **Communication Links:** These are the physical or wireless paths that carry data between nodes. They include Ethernet cables, fiber optics, Wi-Fi, and Bluetooth.

Q36. Differentiate between Cellular Network and Adhoc Wireless Network in detail

Cellular Network:
A cellular network is a centralized network structure where communication is managed by base stations (cell towers). Each base station covers a specific area (cell), and nodes (e.g., mobile phones) communicate through these stations.

Adhoc Wireless Network:
An Adhoc Wireless Network is a decentralized structure where nodes communicate directly with each other without the need for a central authority like a base station.

Feature	Cellular Network	Adhoc Wireless Network
Infrastructure	Requires fixed infrastructure (e.g., base stations)	No fixed infrastructure, fully decentralized
Communication	Through base stations	Direct peer-to-peer or multi-hop routing
Topology	Fixed, determined by base station placement	Dynamic, changes with node mobility
Scalability	Limited by infrastructure capacity	Highly scalable with more nodes
Range	Larger, determined by the base station coverage	Shorter, dependent on node proximity
Routing	Centralized routing through the base station	Decentralized, nodes determine routing paths
Mobility Handling	Managed via handoff between base stations	Managed by dynamic routing protocols
Security	Generally more secure due to centralized control	More vulnerable to security threats like eavesdropping and attacks
Latency	Lower latency due to dedicated infrastructure	Higher latency, especially in larger networks with multi-hop routing