UNIT IV MOBILE NETWORK LAYER

Mobile IP, DHCP, Ad-Hoc, Proactive and Reactive Routing Protocols, Multicast Routing, Vehicular Ad Hoc networks (VANET), MANET Vs VANET, Security Issues

CO4: Interpret the functionality of network layer and identify a routing protocol for a given Ad-hoc networks.

Mobile IP

In the typical diagram of Mobile IP, the mobile node is usually shown moving between two different networks: the home network on the left side and the foreign network on the right. In the home network, a home agent is drawn as a router connected to the mobile node's permanent home address. This part of the diagram represents the original location of the mobile device. The home agent has an arrow pointing toward the permanent home address of the mobile node to show that the device logically still belongs to this network, even if it is physically absent.

When the mobile node moves away from its home network, the diagram shows it entering a different network called the foreign network. Here, another router is shown, labelled as the foreign agent. A temporary IP address, known as the care-of address, is usually written next to this foreign agent to indicate that it represents the mobile node's current position. A dotted or curved arrow from the mobile node to the foreign agent illustrates the mobile node connecting to this foreign network and obtaining the care-of address. In many diagrams, a registration arrow is drawn from the mobile node (or the foreign agent) toward the home agent, showing that the mobile node informs the home agent about its new care-of address. Another arrow coming back from the home agent indicates the approval of this registration.

Fig: 1, shows a correspondent node in the network sending packets to the mobile node. These packets are directed to the mobile node's permanent home address, so the arrows are drawn first toward the home agent. The home agent in the diagram encapsulates these packets, and this is usually shown by drawing a tunnel, often represented by a long curved or straight arrow connecting the home agent to the foreign agent.

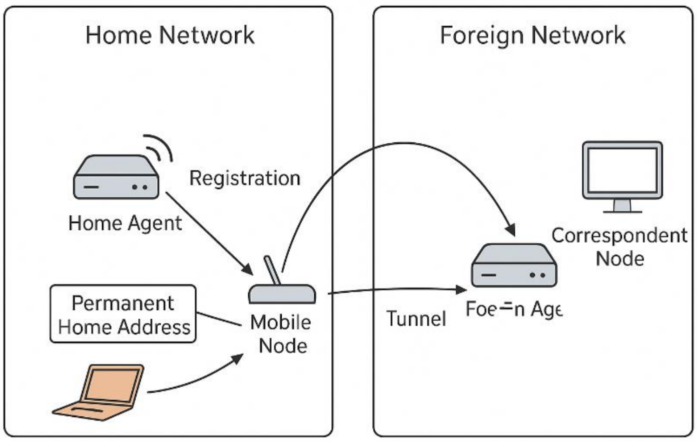


Fig:1 Mobile IP network

This tunnel indicates that the home agent takes the incoming packets, wraps them inside another IP packet, and sends them through this virtual tunnel to the care-of address in the foreign network. At the foreign network end of the tunnel, the foreign agent is shown decapsulating the packet and delivering it to the mobile node, which is depicted with a simple arrow from the foreign agent to the mobile node.

To represent the return path, the diagram usually shows a direct arrow from the mobile node to the correspondent node, illustrating that packets travelling from the mobile node do not need to go back through the home agent. This creates the triangular routing pattern commonly highlighted in Mobile IP diagrams, where one side of the triangle represents packets going from the correspondent node to the home agent, another side represents the tunnel from the home agent to the foreign agent, and the final side represents the direct path back from the mobile node to the correspondent node. This visual triangular shape helps explain the inefficiency of Mobile IP routing.

Dynamic Host Configuration Protocol (DHCP)

It is a network management protocol used to automatically assign IP addresses and essential network configuration parameters to devices on a network. In traditional networks, IP addresses had to be configured manually, which made network administration slow, error-prone, and difficult to scale. DHCP solves this problem by enabling devices to obtain configuration information dynamically and automatically as soon as they join a network. As a result, the user does not need to manually enter parameters such as the IP address, subnet mask, default gateway, or DNS server.

DHCP works on a client–server model. The device that needs an IP address is called the DHCP client, while the server that provides addresses is called the DHCP server. When a new device connects to a network, it does not know its IP address, so it sends a broadcast message across the network requesting configuration. This begins the standard DHCP process known as **DORA**, which stands for Discover, Offer, Request, and Acknowledgment. The process ensures that the device receives an available IP address and the necessary network settings without user intervention.

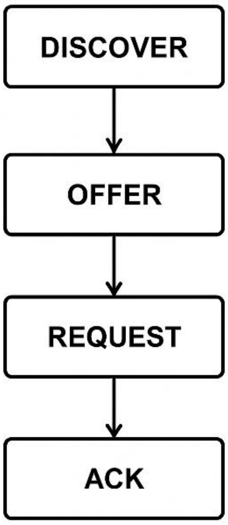


Fig: Process Diagram

The process begins with the **Discover** stage, where the client broadcasts a DHCP Discover message to locate available DHCP servers. Any DHCP server that receives this message responds with a **DHCP Offer**, which includes an available IP address and additional configuration details. The client then chooses one offer—usually the first one it receives—and sends back a **DHCP Request** message indicating its acceptance. The DHCP server finalizes the allocation by replying with a **DHCP Acknowledgment**, officially assigning the IP address to the client for a specific period called a lease. This lease mechanism ensures efficient management of limited IP address pools, especially in large networks with many devices joining and leaving.

DHCP provides more than just IP addresses. It can deliver multiple configuration parameters, known as DHCP options. These include the subnet mask, default gateway, domain name, DNS servers, WINS servers, NTP servers, and many more. By centrally providing all this information, DHCP simplifies network administration and ensures consistency across all devices.

Another important aspect of DHCP is the concept of **address allocation methods**, which include automatic allocation, dynamic allocation, and manual allocation. In automatic allocation, a device receives a permanent IP address that never changes. In dynamic allocation, addresses are leased temporarily and may change over time, making it ideal for networks with many transient devices like schools or public Wi-Fi. Manual allocation binds a device's MAC address to a specific IP address, ensuring that the same device always receives the same IP. This is commonly used for servers, printers, and network devices that require stable addressing.

DHCP also includes a mechanism called **DHCP Relay**. In large networks, it is inefficient to place a DHCP server in every subnet. Instead, a relay agent can forward DHCP messages between subnets, allowing a single DHCP server to serve multiple networks. This makes network design simpler and reduces administrative overhead.

Although DHCP is convenient, it introduces certain limitations. Since IP addresses are assigned automatically, misconfigured servers or unauthorized "rogue" DHCP servers can cause network disruptions by handing out incorrect address information. DHCP also does not provide authentication by default, meaning it trusts any device that joins the network. Because of this, some networks combine DHCP with security mechanisms such as port security, 802.1X authentication, or DHCP snooping.

Advantages

- Automatically assigns IP addresses, reducing manual configuration work
- Minimizes configuration errors such as duplicate IPs or incorrect subnet masks

- Ideal for large networks due to centralized administration
- Supports dynamic address allocation with flexible lease times
- Allows easy addition of new devices—plug-and-play connectivity
- Reduces administrative overhead and saves time
- Supports DHCP options (DNS, gateway, subnet mask, etc.) for complete configuration
- Enhances address utilization efficiency through leasing
- Simplifies network changes and device relocation

Disadvantages

- Devices may receive different IP addresses after lease expiration
- Not suitable for devices that require a fixed IP (servers, printers) without reservation
- Rogue or unauthorized DHCP servers can disrupt network operations
- DHCP relies on broadcasts, which may not pass through routers without relay agents
- Operation fails if the DHCP server becomes unavailable
- Slight delay in network connection because of the DORA process
- No built-in authentication, making it vulnerable to spoofing without additional security

DHCP Vs Static IP

Feature	DHCP	Static IP
IP Assignment	Automatic	Manual
Administration	Centralized and simple	Time-consuming, error-prone
IP Consistency	IP may change after lease refresh	IP always remains the same
Best For	Dynamic/large networks (Wi-Fi, offices, schools)	Servers, routers, printers, CCTV
Scalability	Highly scalable	Difficult in large networks
Configuration Time	Very fast	Slow, must be done per device
Risk of IP Conflicts	Almost none (automatic management)	Higher risk if not tracked properly

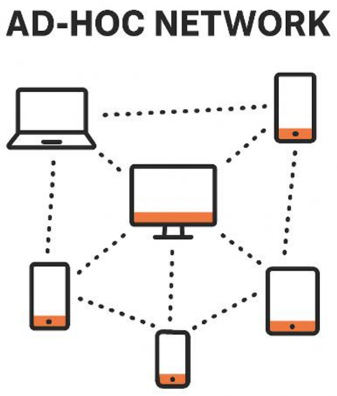
Dependence on Server	Depends on DHCP server	No dependency
Mobility Support	Excellent for devices joining/leaving networks	Not flexible for mobile devices

Ad-Hoc Network

An ad-hoc network is a decentralized type of wireless network where devices communicate directly with each other without relying on any fixed infrastructure such as routers, access points, or base stations. The term “ad-hoc” refers to the spontaneous, temporary, and self-organizing nature of this network. Each device in an ad-hoc network acts as both a host and a router, meaning it can send and receive data while also forwarding packets to other devices. This allows the network to operate independently and dynamically, even in environments where no pre-existing communication infrastructure is available.

Ad-hoc networks are formed automatically when devices come into proximity. For example, laptops, mobile phones, or sensors can detect each other and establish a connection without requiring a central authority. Because the nodes are mobile and free to move in any direction, the network topology changes frequently. This makes ad-hoc networks highly flexible but also challenging to manage, as routing protocols must continuously adapt to changing paths. Popular routing protocols designed for ad-hoc networks include AODV (Ad-hoc On-demand Distance Vector), DSR (Dynamic Source Routing), and OLSR (Optimized Link State Routing), each handling route discovery and maintenance in its own way.

One of the key characteristics of ad-hoc networks is their ability to operate in remote or emergency situations where traditional infrastructure is damaged, unavailable, or impractical. For example, ad-hoc networks are commonly used in disaster recovery operations, military battlefield communications, vehicular networks, and temporary event setups. They are also used in sensor networks and IoT applications where large numbers of small devices need to communicate cooperatively.



Since the devices themselves manage routing, ad-hoc networks face several technical challenges. The lack of a centralized management system makes security more complex, as each node must be trusted to forward data correctly. Nodes may have limited battery power, which affects network performance since forwarding packets consumes energy. Additionally, frequent topology changes due to node mobility can cause route breaks, leading to delays, dropped packets, or reduced throughput.

Key Characteristics

1. Infrastructure-less

There is **no central authority**. Unlike traditional Wi-Fi, which depends on an access point, nodes here connect peer-to-peer.

2. Dynamic Topology

Devices may frequently join, leave, or move within the network. As a result, the network layout constantly changes.

3. Multi-Hop Communication

If two nodes are not within direct wireless range, the data can travel **through intermediate nodes**, making the network extend beyond point-to-point communication.

4. Self-Configuring & Self-Healing

Nodes automatically configure network parameters and reorganize routing paths when a node disconnects or moves away.

5. Limited Range & Resources

Because each device is battery-powered with limited transmission capability, the network performance depends heavily on device energy and position.

Types of Ad-Hoc Networks

i. **Mobile Ad-Hoc Networks (MANETs)**
Composed of mobile devices like smartphones, laptops, or tablets. The topology frequently changes due to mobility.

ii. **Vehicular Ad-Hoc Networks (VANETs)**
Cars, traffic signals, and roadside units communicate to exchange safety and traffic information.

iii. **Wireless Sensor Networks (WSN)**
Small devices (sensors) monitor environmental conditions and forward collected data through neighboring sensors.

iv. **Smart/IoT Ad-Hoc Networks**
Home appliances or smart devices form temporary mesh networks without requiring the internet.

Advantages

- No infrastructure needed → Useful in places lacking network setup.
- Easy and quick to deploy during emergencies or temporary events.
- Cost-effective because no routers or access points are required.
- Flexible and scalable due to easy addition and removal of nodes.
- Supports mobility, allowing devices to move freely without breaking communication.

Disadvantages

- Limited range because communication depends on device signal strength.
- Low security as there is no central authority for authentication.
- Unstable connections due to frequent topology changes.
- Lower bandwidth and high latency, especially in multi-hop communication.
- Power consumption issues as devices act as routers and drain battery faster.
- Complex routing because paths must be continuously updated when nodes move.

Proactive and Reactive Routing Protocols

Routing protocols in ad-hoc networks are designed to handle frequent topology changes and dynamic movement of nodes. Based on how they maintain routing information, these protocols fall into two major categories:

1. Proactive Routing Protocols (Table-Driven)

Proactive routing protocols **continuously maintain up-to-date routing information** for every node in the network. Each node keeps one or more routing tables and regularly exchanges updates with neighbours, even when no communication is taking place. As a result, a route to any destination is always available.

In proactive routing, each node periodically sends routing information packets to every other node. These updates help maintain a complete map of the network. So, when a node wants to send data, it immediately knows the path because it is already stored in the routing table. This leads to **low latency** but increases **overhead** due to constant message exchange.

Advantages

- **Low delay**: Route is immediately available when needed.
- **Consistent routing information** because tables are always updated.
- **Good for real-time applications** where quick response is required.

Disadvantages

- **High overhead** due to periodic updates.
- **Consumes more bandwidth** even when no data is sent.

- **Not efficient** for large or highly dynamic networks because tables change rapidly.

Examples of Proactive Protocols

- DSDV (Destination-Sequenced Distance Vector)
- OLSR (Optimized Link State Routing)
- WRP (Wireless Routing Protocol)

2. Reactive Routing Protocols (On-Demand)

Reactive routing protocols **discover routes only when needed**. Instead of maintaining a full routing table, nodes create a route only when they want to send data. This reduces control overhead but increases delay during route discovery.

When a node has data to send, it initiates a **route discovery process** by broadcasting a Route Request (RREQ). Other nodes forward this request until it reaches the destination or a node with a valid route. The destination responds with a Route Reply (RREP). Once the path is set, data transmission begins. If a link breaks, an error message triggers another route discovery.

Advantages

- Low overhead because no periodic updates are required.
- Saves bandwidth and battery, nodes communicate only when necessary.
- Scalable for large, highly dynamic networks.

Disadvantages

- High initial delay due to route discovery.
- Flooding of RREQ packets may cause congestion.
- Route breaks are more common due to node movement.

Examples of Reactive Protocols

- AODV (Ad hoc On-Demand Distance Vector)
- DSR (Dynamic Source Routing)
- TORA (Temporally Ordered Routing Algorithm)

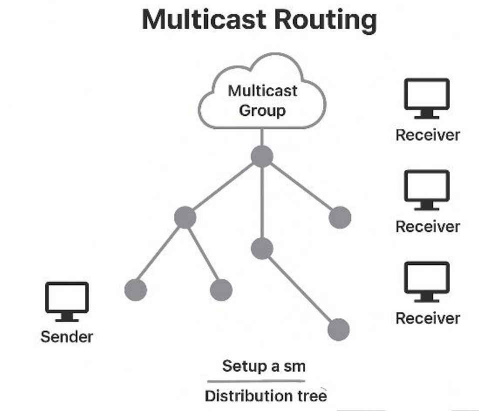
Difference Between Proactive and Reactive Routing Protocols

Feature	**Proactive**	**Reactive**
Route Availability	Always available	Only created when needed
Control Overhead	High (periodic updates)	Low (on-demand)
Latency	Very low	Higher (due to discovery)
Bandwidth Usage	More	Less
Best For	Small or static networks	Large or highly dynamic networks
Examples	DSDV, OLSR	AODV, DSR

Multicast Routing

It is a network routing technique used to send data from one sender to multiple selected receivers simultaneously. Instead of sending individual copies of the data to each receiver (as in unicast), multicast sends a single stream that gets replicated only where necessary in the network. This makes multicast highly efficient for group communication applications such as video conferencing, online lectures, IPTV, and real-time data distribution.

In multicast routing, receivers who want to join a particular data stream become members of a multicast group. Groups are identified using special multicast IP addresses (typically ranging from 224.0.0.0 to 239.255.255.255 in IPv4). These group members may be located anywhere across the network, and they can join or leave the group at any time. The routing system must be able to adapt to these changes dynamically.



The main goal of multicast routing is to build efficient distribution trees that reach all group members while minimizing bandwidth consumption. Instead of sending redundant packets along multiple paths, the routers replicate data only at branching points. This is usually achieved through specialized routing algorithms that maintain information about which interfaces lead to active group members.

Key Concepts in Multicast Routing

1. Multicast Group

- A logical group of receivers who want to receive the same data.
- Identified by a multicast IP address.
- Receivers can freely join or leave the group.

2. Multicast Distribution Tree

- The path along which multicast traffic flows.
- Two types:
  - Source-based Tree (Shortest Path Tree – SPT)
  - Shared Tree (Rendezvous Point Tree – RPT)

3. IGMP (Internet Group Management Protocol)

- Used between hosts and routers.
- Allows devices to join or leave multicast groups.

4. Efficient Bandwidth Usage

- Data is copied only where paths split.
- Avoids sending multiple separate unicast streams.

Types of Multicast Routing Approaches

1. Source-Based Trees (Shortest Path Trees – SPT)

- A separate tree is created from each source to all receivers.
- Uses shortest path algorithms like Dijkstra.
- Very fast delivery but high state information in routers.

2. Shared Trees

- A single common tree is used for all sources.
- Built around a central router called a Rendezvous Point (RP).
- Reduces router memory consumption but may not provide optimal shortest paths.

3. Flood-and-Prune (Dense-Mode Multicast)

- Assumes receivers are everywhere.
- Routers initially flood traffic across the network.
- Unwanted branches are later pruned.
- Good for dense networks.

4. Explicit Join (Sparse-Mode Multicast)

- Assumes receivers are in few places.
- Routers forward multicast traffic only when they receive explicit join messages.
- More efficient for large networks.

Multicast Routing Protocols

1. DVMRP (Distance Vector Multicast Routing Protocol)

- Based on Distance Vector routing.
- Uses flood-and-prune (dense mode).

2. PIM (Protocol Independent Multicast)

Two main modes:

- PIM-DM (Dense Mode) → Flood-and-prune
- PIM-SM (Sparse Mode) → Uses a shared tree with an RP

3. MOSPF (Multicast Open Shortest Path First)

- Extension of OSPF.
- Uses link-state information to form multicast trees.

Advantages

- Efficient use of bandwidth, sends one stream to many.
- Reduced network load compared to unicast.
- Supports real-time applications (live video, gaming).
- Dynamic membership management (users can join/leave anytime).
- Scalable for large group communication.

Disadvantages of Multicast Routing

- Complex to implement and manage.
- Requires multicast-capable routers and protocols.
- Security issues, hard to authenticate group members.
- Not widely used in public internet (mostly supported in private networks).
- Routing algorithms can be resource-intensive.

Applications of Multicast Routing

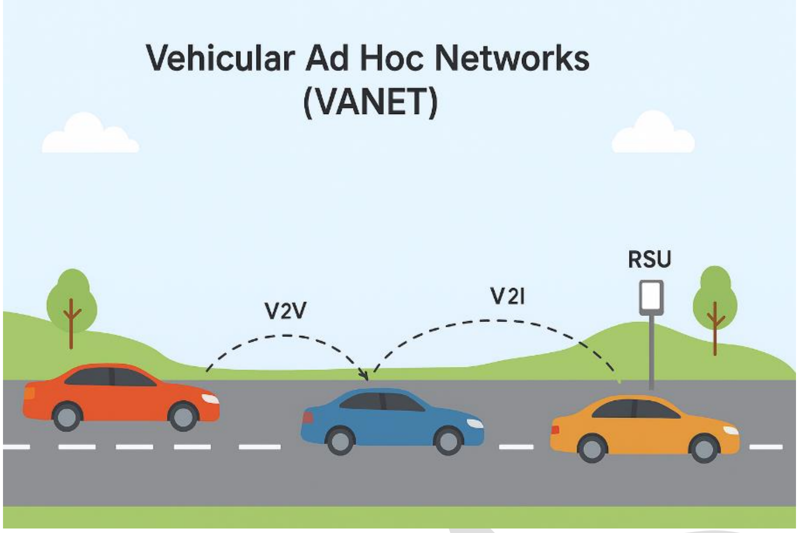
- IPTV and live video streaming
- Webinars and online classroom broadcasts
- Military communication systems
- Real-time stock market data distribution
- Multiplayer online gaming
- Distributed simulations

Vehicular Ad Hoc Networks (VANETs)

It represents a specialized form of mobile ad hoc networks designed exclusively for communication between vehicles and between vehicles and roadside infrastructure. In a VANET, every vehicle is equipped with wireless communication hardware, onboard sensors, and GPS systems, which allow it to function as an intelligent mobile node within a constantly changing network environment. As vehicles move along roads and highways, they automatically discover other nearby vehicles and establish temporary communication links without requiring any fixed centralized infrastructure. This ability to organize and reorganize communication autonomously makes VANETs extremely useful for modern Intelligent Transportation Systems (ITS).

One of the most defining features of a VANET is the high mobility of its nodes. Vehicles travel at high speeds and often in different directions, which causes the network topology to change rapidly within seconds. As a result, communication links are frequently created and broken, making VANETs one of the most dynamic types of wireless networks. Despite this rapid movement, vehicle mobility patterns are still somewhat predictable because vehicles generally follow road layouts, traffic rules, and speed regulations. This predictable movement helps network designers create efficient routing and communication mechanisms tailored for transportation environments.

VANET communication mainly operates in two forms: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In V2V communication, vehicles directly exchange information such as position, speed, acceleration, and sudden braking signals. This direct exchange plays a vital role in preventing accidents, as vehicles can react to dangerous situations much faster than human drivers. In V2I communication, vehicles interact with roadside units (RSUs), such as traffic signals, toll booths, or traffic management centers. These RSUs can broadcast important messages like traffic congestion updates, roadwork warnings, weather alerts, and emergency notifications. The combination of V2V and V2I communication creates a cooperative driving environment in which both vehicles and infrastructure contribute to safer and more efficient transportation.



VANET applications can be broadly classified into safety-related, traffic management, and comfort-oriented categories. Safety applications form the backbone of VANET technology. These include collision avoidance alerts, lane-change warnings, blind spot detection, and emergency vehicle notifications. Such applications allow drivers to receive real-time, location-specific warnings that can save lives. Traffic management applications, on the other hand, focus on improving overall road efficiency by providing real-time traffic congestion information, optimal route suggestions, and intelligent traffic light coordination. This helps reduce travel times, fuel consumption, and environmental pollution. Comfort and infotainment applications enhance the traveling experience by offering Internet access, entertainment services, location-based advertisements, and navigation assistance.

Although VANETs offer numerous benefits, they also face several challenges. One of the biggest challenges is maintaining stable communication in a highly dynamic environment. Because vehicles are constantly moving at high speeds, routing protocols must quickly adapt to changing conditions and ensure that messages reach their intended destination in time. Another important challenge is security. VANETs carry sensitive information such as vehicle identity, location, and driving patterns. If unauthorized users intercept or manipulate these messages, it can lead to dangerous situations, privacy violations, or malicious attacks. Therefore, strong encryption, authentication mechanisms, and privacy-preserving methods are essential components of VANET architecture. Additionally, the deployment of VANETs requires significant investment in roadside infrastructure such as sensors, communication units, and traffic management systems, which may not be affordable in all regions.

Characteristics of VANETs

1. **High Mobility**: Vehicles move at high speeds, causing rapid changes in network topology. Connections between nodes frequently form and disappear.
2. **Dynamic Topology**: Because vehicles move in different directions and at variable speeds, the network structure changes continuously and unpredictably.
3. **Distributed Architecture**: VANETs do not rely on a central controller. Instead, communication happens peer-to-peer or through roadside infrastructure.
4. **Large-Scale Deployment**: VANETs may span entire cities or highways, covering very large geographical areas.
5. **Predictable Mobility Patterns**: Although mobility is high, vehicle movement follows roads and traffic rules, making mobility somewhat predictable.
6. **Frequent Disconnections**: Due to rapid movement and varying vehicle density, network connections may break often.
7. **Real-Time Communication**: VANET applications often require very low latency for safety messaging, such as collision warnings.

Types of VANET Communication

1. **Vehicle-to-Vehicle (V2V)**: Direct communication between nearby vehicles to share safety alerts, speed data, or traffic updates.
2. **Vehicle-to-Infrastructure (V2I)**: Vehicles communicate with roadside units (RSUs) for traffic signals, toll information, or weather updates.
3. **Infrastructure-to-Vehicle (I2V)**: Roadside units send information back to vehicles, such as road closure alerts.

4. **Vehicle-to-Pedestrian (V2P)**: Communication between vehicles and mobile devices carried by pedestrians or cyclists.

Applications of VANETs

1. Safety Applications

- Collision warning systems
- Lane-change assistance
- Emergency vehicle notifications
- Blind spot detection
- Sudden brake alerts

These applications aim to reduce accidents and improve road safety by enabling vehicles to react faster than humans.

2. Traffic Management Applications

- Real-time traffic congestion updates
- Dynamic route planning
- Smart traffic light coordination
- Parking availability systems

These applications help reduce travel time and fuel consumption.

3. Comfort and Infotainment Applications

- Internet access
- Location-based advertisements
- Media streaming
- Weather and navigation updates

Such features enhance the driving experience for passengers.

4. Commercial Applications

- Fleet management

- Automated toll collection
- Usage-based insurance models

Advantages of VANETs

- Improved Road Safety: Real-time alerts help avoid accidents.
- Efficient Traffic Flow: Reduces congestion through intelligent traffic control.
- Enhanced Driving Experience: Provides entertainment and useful travel information.
- Scalability: Can operate across city-wide or nation-wide transportation networks.
- Decentralization: Reduces dependence on centralized servers.

Challenges and Limitations

- High Mobility Issues: Rapid topology changes complicate routing.
- Network Congestion: High traffic density may overwhelm communication channels.
- Security Threats: Risks include message tampering, spoofing, and cyber-attacks.
- Privacy Concerns: Tracking vehicle movement may reveal personal data.
- Infrastructure Costs: Installing roadside units and sensors is expensive.
- Connectivity Fluctuations: Sparse vehicle density areas may face communication gaps.

Routing in VANETs

Routing is significantly challenging due to mobility. Common routing approaches include:

1. Topology-Based Routing

Uses information about network links.

- Proactive (e.g., table-driven)
- Reactive (e.g., on-demand)

2. Position-Based Routing

Uses GPS location information to route packets efficiently.

3. Cluster-Based Routing

Vehicles form clusters to maintain stable communication structures.

MANET Vs VANET

Feature	MANET (Mobile Ad Hoc Network)	VANET (Vehicular Ad Hoc Network)
Definition	A general wireless ad hoc network formed by mobile devices without fixed infrastructure.	A specialized type of MANET formed between moving vehicles and roadside units.
Node Type	Smartphones, laptops, handheld devices, sensors.	Vehicles equipped with onboard units, sensors, and wireless modules.
Mobility Speed	Low to moderate mobility, unpredictable movement.	Very high mobility; vehicles move fast along predefined roads.
Topology Changes	Frequent but relatively manageable.	Extremely rapid and highly dynamic due to fast-moving vehicles.
Energy Source	Battery-powered devices with limited energy.	Vehicles supply ample and continuous power; no major energy constraints.
Communication Pattern	Random movement, multi-hop communication common.	Structured movement; communication is often short-lived due to fast mobility.
Infrastructure Support	Completely infrastructure-less.	May use roadside units (RSUs) in addition to ad hoc links.
Routing Complexity	Moderate; topology changes are slower.	High; routing must adapt quickly to rapid topology shifts.
Primary Applications	Military, disaster recovery, temporary communication, sensor networks.	Traffic safety, collision avoidance, traffic management, infotainment.
Latency Requirement	Moderate; not always time-critical.	Very low latency needed for safety messages and emergency alerts.
Network Size	Small to medium, depending on nodes present.	Very large-scale, covering cities and highways.
Predictability of Movement	Low; nodes move independently.	High; vehicles follow roads, lanes, and traffic rules.
Connectivity Stability	Often unstable due to mobility.	Highly unstable due to high-speed movement and variable traffic density.

Environment	Indoor or outdoor general environments.	Strictly outdoor, road-based environments.

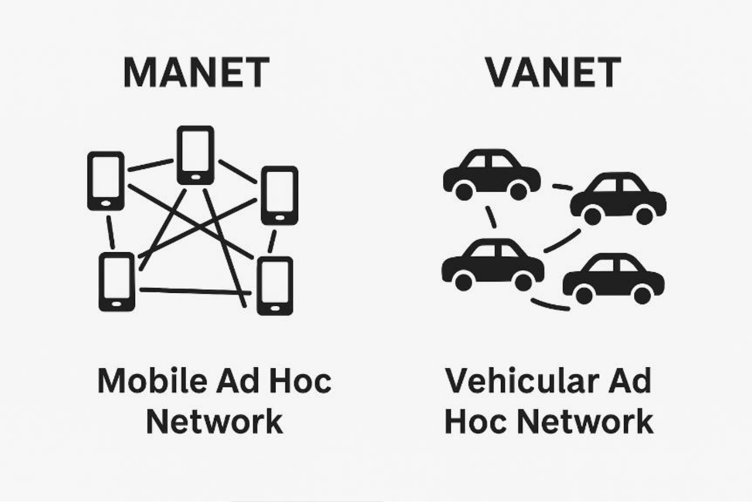


Fig: MANET vs VANET

Security Issues in MANET and VANET

Mobile Ad-Hoc Networks (MANETs) and Vehicular Ad-Hoc Networks (VANETs) are both decentralized, dynamic wireless networks. Because they operate without fixed infrastructure, they face several significant security threats.

Below is a descriptive explanation of the major security issues common to both, followed by issues specific to each.

Common Security Issues in MANET and VANET

(i) Authentication Issues

Since there is no central authority, verifying whether a node is legitimate becomes difficult.
Attackers may impersonate genuine devices and inject false information.

(ii) Confidentiality Breaches

Wireless communication is open to eavesdropping. Sensitive information (location, messages, routing data) can be intercepted by malicious nodes.

(iii) Integrity Attacks

Attackers may modify, alter, or forge packets during transmission. This can mislead routing decisions or cause false alerts in VANETs (e.g., fake accident messages).

(iv) Availability Attacks

Denial of Service (DoS) and jamming attacks make the network unavailable by overwhelming the channel or nodes, disrupting communication.

(v) Secure Routing Challenges

Dynamic topology leads to frequent route changes. Attackers exploit this to inject false routes, drop critical packets, or misdirect traffic.

(vi) Node Capture / Compromise

Nodes can be physically stolen or tampered with. A compromised node becomes an insider threat and can participate in harmful activities undetected.

Security Issues Specific to MANET

(i) Black Hole Attacks

A malicious node advertises the shortest route but drops all received packets.

(ii) Wormhole Attacks

Two attackers create a tunnel to replay packets, disrupting routing.

(iii) Sybil Attack

One node claims multiple identities, confusing routing protocols.

(iv) Lack of Stable Infrastructure

Because node mobility is unpredictable, maintaining secure key management is difficult.

(v) Power Constraints

Nodes often run on battery. Energy-draining attacks (e.g., excessive communication) can shut them down.

Security Issues Specific to VANET

(i) High-Speed Mobility Issues

Vehicles move fast; this causes rapid topology changes, making security protocols harder to maintain.

(ii) Location Tracking & Privacy Risks

Vehicles constantly broadcast their position, enabling attackers to track a driver's movement.

(iii) Message Forgery in Safety Applications

Fake messages such as:

- fake accident warnings
- false traffic congestion alerts
- fake emergency vehicle notices can manipulate driver behaviour, causing accidents or congestion.

(iv) RSU (Roadside Unit) Vulnerability

If RSUs are compromised, they can distribute false information to all vehicles.

(v) Timing Attacks

Delay or replay of safety messages (e.g., braking alerts) may cause accidents.

(vi) GPS Spoofing

Attackers can manipulate navigation signals, misguiding vehicles.