UNIT III - MOBILE NETWORK LAYER

Mobile IP – DHCP – AdHoc– Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV , Hybrid routing –ZRP, Multicast Routing- ODMRP, Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security.

PART - A

1. What is the key mechanism in mobile IP? [Nov 2018]

- **Agent Discovery** - A Mobile Node discovers its Foreign and Home Agents during agent discovery.
- **Registration** - The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.
- **Tunnelling** - A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

2. State the purpose of Home Location Register (HLR). [Nov 2018]

- The Home Location Register (HLR) is the main database of permanent subscriber information for a mobile network.
- The HLR is an integral component of CDMA (code division multiple access), TDMA (time division multiple access), and GSM (Global System for Mobile communications) networks.

3. What is the purpose of DHCP? [Apr 2018]

- DHCP's purpose is to enable individual computers on an IP network to extract their configurations from a server (the DHCP server) or servers, in particular, servers that have no exact information about the individual computers until they request the information.
- The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

4. What is the purpose of agent solicitation message? [Apr 2018]

- In case a mobile node (MN) does not receive any COA, then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation messages do not flood the network.
- A mobile node can usually send up to three solicitation messages (one per second) as soon as it enters a new network. The basic purpose of the solicitation messages sent by a mobile node (MN) is to search for a foreign agent (FA).
- For a highly dynamic wireless network in which MNs move at great speed, even a time interval of the order of a second between these messages is too long.
- If an MN does not receive any address in response to its solicitation messages, then to avoid network flooding, the MN should exponentially reduce the rate of sending the solicitation messages.

5. To which layer do each of the following protocols belong to? What is their functionality? RARP, DNS [Nov 2017]

RARP (Reverse Address Resolution Protocol):

The RARP protocol is used by IP to find the IP address based on the physical (MAC address) address of a computer.

DNS: It stands for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver).

It is a software service available on the Internet that is responsible for translating domain names into IP addresses.

6. Differentiate the functionalities of a foreign agent and home agent. [Nov 2017]

Foreign Agent (FA):

The foreign agent is a router in a foreign network that functions as the point of attachment for a mobile node when it roams to the foreign network. The packets from the home agent are sent to the foreign node which delivers it to the mobile node.

Home Agent (HA):

It is located in home network and it provides several services for the MN. HA maintains a location registry. The location registry keeps track of the node locations using the current care-of-address of the MN.

7. What is Route Optimization? [May 2017]

- Route Optimization is the process of determining the most cost-efficient route.
- It's more complex than simply finding the shortest path between two points.
- It needs to include all relevant factors such as the number and location of all the required stops on the route.

8. List the modifications proposed in single-hop and multi-hop wireless network. [May 2017]

Single hop network:

In a single hop network , when a packet leaves the source it just takes a single hop (goes through another network or you can say it passes through another router from a different network) before reaching its destination address.

Multi-hop network:

In a multi-hop network a packet has to go through 2 or more networks in order to reach its destination address.

While taking a hop through a different network a packet may go through various devices like Routers, network bridges, switches, etc.

9. Define COA. [Nov 2016]

- Used in Internet routing, a care-of address (usually referred to as *CoA*) is a temporary IP address for a mobile device.
- This allows a home agent to forward messages to the mobile device.
- A separate address is required because the IP address of the device that is used as host identification is topologically incorrect - it does not match the network of attachment.

- The care-of address splits the dual nature of an IP address, that is, its use is to identify the host and the location within the global IP network.

10. Illustrate the use of BOOTP protocol? [Nov 2016]

The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

11. What is DHCP? [May 2016]

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

12. What is encapsulation in mobile IP? [May 2016]

- Encapsulation describes the process of placing an IP datagram inside a network packet or frame.
- Encapsulation refers to how the network interface uses packet switching hardware

13. Define Tunnelling with its functions?

- The packet is forwarded by the home agent to the foreign agent. When the packet comes to the foreign agent (care-of-address), it delivers the packet to the mobile node. This process is called **tunnelling.**
- Tunnelling has two primary functions:
  1. Encapsulation of the data packet to reach the tunnel endpoint,
  2. Decapsulation when the packet is delivered at that endpoint.

14. Define Care-Of-Address (COA) with its types?

- **Care-of-Address (COA):** It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.
- The COA can be any of the following two types:
  (a) Foreign agent COA: The COA is an IP address of foreign agent (FA).
  (b) Co-located COA: When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

15. Define Agent Discovery and its discovery methods?

- **Agent Discovery:** During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as **agent discovery.**
- The following two discovery methods are popularly used:
  (1) Agent advertisement and (2) Agent solicitation.

16. Describe some of the features of Mobile IP

- **Transparency:** The IP address is to be managed transparently and there should not be any effect of mobility on any ongoing communication.

- **Compatibility:** Mobile IP should be compatible with the existing Internet protocols.
- **Security:** Mobile IP should, as far as possible, provide users with secure communications over the Internet.
- **Efficiency and Scalability:** In the event of worldwide support, there can be a large number of mobile systems in the whole Internet. It should also be scalable to support billions of moving hosts worldwide.

17. What are the key mechanisms followed by Mobile IP?

- Mobile IP is associated with the following three basic mechanisms:
  1. Discovering the care-of-address
  2. Registering the care-of-address
  3. Tunnelling to the care-of-address

18. Mention the two main design issues of MANET? [Nov 2018]

- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

19. What are the important steps in destination sequence distance vector routing? [Nov 2018]

- Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm.
- The main contribution of the algorithm was to solve the routing loop problem.
- Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used.
- The number is generated by the destination, and the emitter needs to send out the next update with this number.
- Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

20. Compare VANET and MANET? [Apr 2018]

- MANET is the short form of Mobile AdHoc Network. In ad-hoc networks all the nodes are mobile in nature and hence they can be interfaced dynamically in arbitrary fashion.
- While VANET is the short form of Vehicular Adhoc Network. It is sub-class of network of MANET type.

21. Differentiate cellular with adhoc networks? [Apr 2018]

Parameters	Cellular network	Ad Hoc network

Network routing	Centralized, all the traffic goes through the Base Station	Distributed, No centralized system such as Base station needed
Switching Type	Circuit Switching	Packet Switching
Number of Hops	single hop type	Multiple hops
Topology	Star	Mesh
Application	Designed and developed for voice traffic	Designed to meet best effort data traffic requirements
Cost and time for installation	Higher cost and takes more time for deployment	Lower cost and does not take more time for deployment
Call drops	Low call drops during mobility due to seamless connectivity across region	Higher breaks in the path during mobility
Network maintenance	requires periodic maintenance and hence it is costly.	nodes are self organising and hence it is less costly.
Frequency re-use	It utilizes same frequency channels in the nearby cells with proper RF planning and antenna placement. This is known as static frequency re-use.	Dynamic frequency re-use is employed using carrier sense mechanism.
Bandwidth (BW) mechanism	The allocation of BW is guaranteed and easy.	The allocation of BW is based on shared channel using complex MAC algorithms.
Technologies	IS-95, IS-136, GSM, Mobile WiMAX, CDMA, LTE	WLAN 802.11e

22. List the applications of MANET's. [May 2017]

- Communication among portable computers
- Environmental monitoring
- Military

- Emergency applications

23. Distinguish proactive and reactive protocols. [May 2017]

Proactive: A table -driven approach, follows a static route through out the lifetime.
Reactive: Dynamically changes the Routing decisions based on the present network conditions.

24. Compare AODV and DSR protocols. [Nov 2017]

- Adhoc on-demand routing protocol (AODV) and Dynamic Source Routing (DSR) under different performance metrics like throughput, packet drop rate and end-to-end delay.
- AODV protocol is better than DSR protocol as the nodes are increasing/adding to network. Packet drop rate and end-to-end delay of AODV protocol is less than DSR protocol as the nodes are increasing.

25. What are the contents of Link state Advertisement message?[Nov 17]

A link state advertisement message contains:

- The identity of the router originating the message.
- The identities of all its neighbours.
- The delays along various links to its neighbours.

26. Outline the concept of RTT? [Nov 2016]

- Round-trip time (RTT), also called round-trip delay, is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.
- In this context, the source is the computer initiating the signal and the destination is a remote computer or system that receives the signal and retransmits it.

27. Compare and contrast MANET Vs VANET [Nov 2016]

Compare MANET Vs VANET. [May 2016]

- These networks are used for communication between following: between vehicles and road-side infrastructure.
- MANET is the short form of Mobile AdHoc Network. In ad-hoc networks all the nodes are mobile in nature and hence they can be interfaced dynamically in arbitrary fashion.
- **VANET** is the short form of Vehicular Adhoc Network. It is subclass of network of MANET type. In VANET, the communication nodes are moving on pre-defined roads as finalized initially.

28. List the characteristics of MANETs. [May 2016]

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.

- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

29. What is Adhoc Network?

Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

30. What is Mobile Adhoc Network?

A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.

31. What are the characteristics of MANET?

- Lack of fixed infrastructure
- Dynamic topologies
- Bandwidth constrained, variable capacity links
- Energy constrained operation
- Increased vulnerability

32. What are the types of traffic?

The common traffic types are the following:

- Bursty traffic
- Large packets sent periodically
- Combination of the above two types of traffic

33. What are the three important ways in which a MANET routing protocol differs from routing of packets in a traditional network?

1. In a MANET, each node acts as a router, whereas ordinary nodes in a traditional wired network do not participate in routing the packets.
2. In a MANET, the topology is dynamic because of the mobility of the nodes, but it is static in the case of traditional networks. Thus, the routing tables in a MANET quickly become obsolete, making the routing process complicated.
3. In the simple IP-based addressing scheme deployed in wired networks, the IP address encapsulated in the subnet structure does not work because of node mobility.

34. What are the types of communications?

- *Unicast:* In this, a message is sent to a single destination node.
- *Multicast:* In this type of transmission, a message is sent to a selected subset of the network nodes.
- *Broadcast:* In this type of transmission, a message is sent to all the nodes in the network.

35. What are the types of popular MANET routing protocols?

1. Destination-Sequenced Distance-Vector Routing Protocol
2. Dynamic Source Routing (DSR) Protocol
3. Ad Hoc On-demand Distance Vector (AODV)
4. Zone Routing Protocol(ZRP)
5. Multicast Routing Protocols for MANET

36. What is tree based protocol?

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

37. What is mesh based protocol?

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.

The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

38. Define VANET.

- Vehicular Adhoc Network.
- A Vehicular Ad Hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- A vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.
- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.

39. What are the characteristics of secure Adhoc Network?

A secure ad hoc network should have the following characteristics:

Availability: It should be able to survive denial-of-service (DoS) attacks.

Confidentiality: It should protect confidentiality of information by preventing its access by
unauthorized users.

Integrity: It should guarantee that no transferred message has been tampered with.

Authentication: It should help a node to obtain guarantee about the true identity of a peer node.

Non-repudiation: It should ensure that a node having sent a message, cannot deny it.

40. What are the two phases of DSR?

1. Route discovery
2. Route maintenance

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.
- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.

41. What is the use of VANET?

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

42. What is network topology?

The topology of a network denotes the connectivity among the various nodes of the network.

43. What are the classification of Unicast MANET Routing Protocols?

- Unicast routing protocols in MANETs are classified into **proactive** (table-driven), **reactive** (ondemand) and **hybrid protocols**.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

44. Draw a schematic model of a Mobile Adhoc Network.

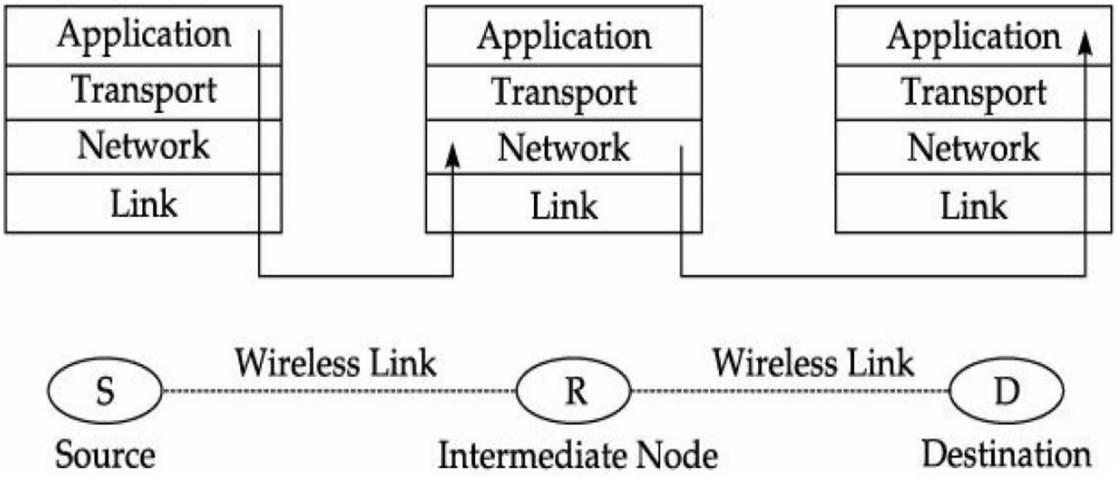


Figure 7.1 *A schematic model of a mobile ad hoc network.*

45. What is proactive protocol?

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- In this protocol, each node in a routing table maintains information about routes to every other node in the network.
- These tables are periodically updated in the face of random network topology changes. An example of a proactive (table-driven) protocol is the Destination Sequenced Distance Vector (DSDV) protocol.

46. What is reactive protocol?

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not maintain up-to-date routes to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.

Two examples of on-demand routing protocols are:
(i) Dynamic source routing (DSR)
(ii) Ad hoc on-demand distance vector routing (AODV)

PART-B

1. What is mobile IP? Explain various entities and terminologies used in Mobile Systems. (Or) Explain the services of Mobile IP and describe the tunneling process?

Explain mobile IP requirement and terminologies. (8) [Nov 2018]

Illustrate packet delivery mechanism in mobile IP network with a neat diagram. (16) [Nov 2017]

With a neat diagram explain how packet delivery to and from a mobile node is transferred in mobile IP. (16) [May 2017]

Mobile Internet Protocol

Key Points

- Correspondent node (CN)
- Mobile Node (MN)
- Home agent (HA)
- Foreign Agent (FA)
- Home Network (HN)
- Foreign Network (FN)
- Care-of-Address (COA)
- Agent discovery
  - Agent advertisement, and
  - Agent solicitation.
- Tunnelling and encapsulation
- Packet Delivery

- The Internet is built on top of a collection of protocols, called the TCP/IP protocol suite. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the core protocols in this suite.
- IP is responsible for routing a packet to any host, connected to the Internet, uniquely identified by an assigned IP address.

- The nodes in the LAN are assigned an address based on the LAN address.
- Mobile Internet Protocol (Mobile IP) was proposed by the Internet Engineering Task Force (IETF).
- Mobile IP is a standard protocol that extends the Internet Protocol by making mobility transparent to applications and to higher level protocols like TCP.

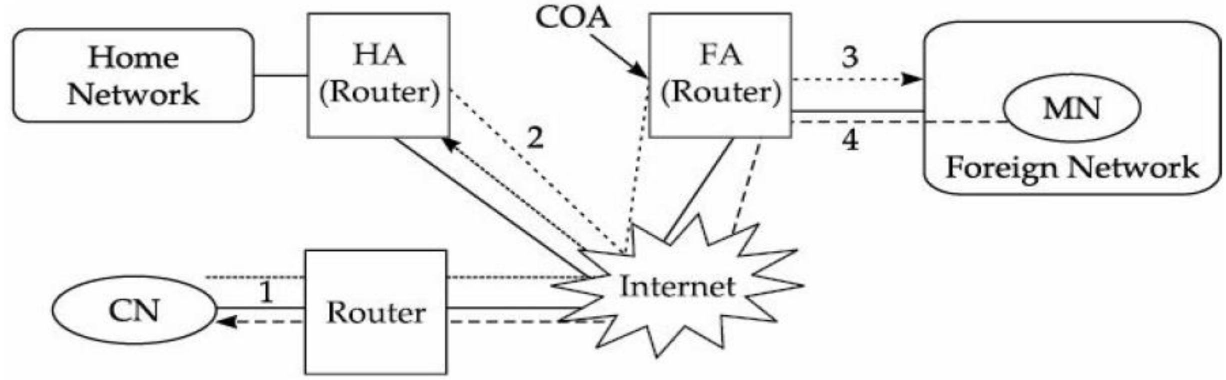


Figure 2.1 Packet deliveries to and from a mobile node.

- Correspondent node (CN) is connected via a router to the Internet, and the home network and the foreign network are also connected via a router, i.e. the home agent (HA) and foreign agent (FA), respectively, to the Internet.
- Home agent (HA) is implemented on the router connecting the home network with the Internet, a foreign agent (FA) is also implemented on the router connecting the foreign network with the Internet.
- The tunnel for the packets towards the mobile node starts at the home agent and ends at the foreign agent, again here the foreign agent has the care-of-address (COA).

Terminologies—Mobile IP

Mobile Node (MN):

A mobile node is hand held equipment with roaming capabilities. It can be a cell phone, personal digital assistant, laptop, etc.

Home Network:

The home network of a mobile device is the network within which the device receives its identifying IP address (home address). In other words, a home network is a subnet to which a mobile node belongs to as per its assigned IP address. Within the home network, there is no need of mobile IP.

Home Address (HA):

The home address of a mobile device is the IP address assigned to the device within its home network. The IP address on the current network is known as home address.

Foreign Agent (FA):

The foreign agent is a router in a foreign network that functions as the point of attachment for a mobile node when it roams to the foreign network. The packets from the home agent are sent to the foreign node which delivers it to the mobile node.

Foreign Network (FN):

The foreign network is the current subnet to which the mobile node is visiting. It is different from home network. In other words, a foreign network is the network in which a mobile node is operating when away from its home network.

Correspondent Node (CN):

The home agent is a router on the home network serving as the anchor point for communication with the mobile node. It tunnells packets from a device on the Internet, called a correspondent node (CN), to the roaming mobile node.

Tunnelling Process
The packet is forwarded by the home agent to the foreign agent. When the packet comes to the foreign agent (care-of-address), it delivers the packet to the mobile node. This process is called **tunnelling.** Tunnelling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint.

Care-of-Address (COA):

It is the address that is used to identify the present location of a foreign agent. The packets sent to the MN are delivered to COA.

The COA can be any of the following two types:

(a) Foreign agent COA: The COA is an IP address of foreign agent (FA).

(b) Co-located COA: When the mobile node (MN) acquires a temporary IP address, that address acts as the COA.

Care-of-Address (COA):
In real life, if a person is not in his own house and living in a temporary location, that location is called his care-of-address (C/O) but, here, the care-of-address defines the current location of the mobile node from an IP point of view. All IP packets sent to mobile nodes are delivered to the care-of-address (COA), i.e. not directly to the IP address of the mobile node.

Note: The co-located address (temporary IP address) can be acquired using services like dynamic host configuration protocol (DHCP).

Home Agent (HA):

It is located in home network and it provides several services for the MN. HA maintains a location registry. The location registry keeps track of the node locations using the current care-of-address of the MN.

Explain the Agent Discovery Process in Mobile IP? (5) [Apr 2018]

Agent Discovery:

During call establishment it is necessary for a mobile node to determine its foreign agent. This task is referred to as **agent discovery.**

The following two discovery methods are popularly used:

(1) Agent advertisement, and
(2) Agent solicitation.

1. Agent advertisement:

- Generally the foreign and the home agents advertise their presence through periodic agent advertisement messages.
- An agent advertisement message, lists one or more care-of-addresses and a flag indicating whether it is a home agent or a foreign agent. Agent advertisement is a popularly used method in agent discovery.

2. Agent solicitation:

- In case a mobile node (MN) does not receive any COA, then the MN should send an agent solicitation message. But it is important to monitor that these agent solicitation messages do not flood the network.
- A mobile node can usually send up to three solicitation messages (one per second) as soon as it enters a new network. The basic purpose of the solicitation messages sent by a mobile node (MN) is to search for a foreign agent (FA).
- For a highly dynamic wireless network in which MNs move at great speed, even a time interval of the order of a second between these messages is too long. If an MN does not receive any address in response to its solicitation messages, then to avoid network flooding, the MN should exponentially reduce the rate of sending the solicitation messages.

Tunnelling and encapsulation

- Tunnelling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint.
- Tunnelling is the process of sending a packet via a tunnel and it is achieved by a mechanism called **encapsulation**. Encapsulation refers to arranging a packet header and data in the data part of the new packet.
- Disassembling the data part of an encapsulated packet is called **decapsulation**. Whenever a packet is sent from a higher protocol layer to a lower protocol layer, the operations of encapsulation and decapsulation usually take place.

Packet Delivery

- Let us consider the situation, where the corresponding node (CN) wants to send an IP packet to a mobile node. CN sends the packet to the IP address of the mobile node as shown in step 1 of Fig. 2.1.
- The IP address of the MN is the destination address, whereas the address of CN is the source address. The packet is passed to the Internet that does not have any information about the MN's current location. So the Internet routes the packet to the router of the MN's home network.
- The home agent examines the packet to determine whether the MN is present in its current home network or not. In case that MN is not present, then the packet is encapsulated by a new header that is placed in front of the existing IP header.
- The encapsulated packet is tunnelled to the COA, which act as the new destination address and the HA acts as the source address of the packet as shown in step 2 of Fig. 2.1
- The encapsulated packet is routed to the foreign agent which performs decapsulation to remove the additional header and forwards the decapsulated packet to the MN, which is the actual destination, as specified by the source node (CN), shown in step 3 of Fig. 2.1.

- The MN after receiving the packet from CN, forwards a reply packet to the CN by specifying its own IP address along with the address of the CN as shown in step 4 of
- The MN's IP address acts as the source address and the CN's IP address acts as the destination address. The packet is routed to the FA. After receiving the packet, FA forwards the packet to CN.

2. Answer the following with respect to missing and duplicate segments in TCP operation.

(a) What can cause segments to be missed at the receiver-end and also cause duplicate segments to arise? Explain your answer using a suitable scenario of operation.

(b) How exactly is a missing segment detected in TCP? Explain the specific actions that take place when a missing segment is detected.

Key Points

- Goal of mobile IP
- Scenario
- Advantages
- Disadvantages
- Desirable Features of Mobile IP

Overview of Mobile IP

The goal of mobile IP is to enable packet transmission efficiently without any packet loss and disruptions in the presence of host and/or destination mobility.

Scenario

- Suppose a person working as a business development executive for a company needs to take care of many regional offices in India and abroad.
- His home office is in Delhi where he spends about 40% of his time. The rest of the time he spends between the other offices, say, Kolkata, Mumbai, Chennai, Kathmandu and Singapore.
- A problem that arises in this context is: how does he make arrangements so that he would continue to receive postal mails regardless of his location? If we can answer this, we can easily understand how IP works in the context of a mobile device.
- There are two broad categories of solutions to this problem being faced by the business executive:

  (i) address changing,

  (ii)decoupling mail routing from his address.
- It would be difficult for the business development executive to inform about his changed address to all those who are likely to write letters to him each time he moves.
- Also, by the time, he would have informed everyone about his new address; it would have become time for the address to change again.
- And he certainly cannot decouple the routing of mail from his address, unless he has set up his own personal postal system.

- A practical solution to this problem is mail forwarding. Let us say that he leaves Delhi for Singapore for a couple of months.
- He will inform the Delhi post office that he will be in Singapore.
- The Delhi post office would intercept his mails headed for his normal Delhi address, reliable them, and forward them to Singapore.
- Depending on where he is staying, this mail might be redirected either straight to a new address in Singapore, or to a Singapore post office where he can pick it up.
- If he leaves Singapore to go to another city, say, Kathmandu, he would just call the Delhi post office and tell them about his new location.
- When he gets back to home office, he will cancel the forwarding arrangement and get his mail as usual.

Advantages

- Simple mechanism to understand and implement.
- This scheme is transparent to everyone sending mails

Disadvantages

- To keep communicating with his home post office each time he moves.
- Every piece of mail has to be sent through the system twice—first to Delhi and then to wherever he moves, which is inefficient and delay in delivering and also loads the postal system.
- The mobile node is normally resident on its home network, which is the one indicated by the network ID in its IP address.
- Devices on the internetwork always route using this address, so the pieces of "mail" (datagrams) always arrive at a router at the device's "home".
- When the device "travels" to another network, the home router ("post office") intercepts these datagram's and forwards them to the device's current address.
- The mobile node's home router serves as the home agent and the router in Singapore as the foreign agent. The mobile has been assigned a temporary "care-of address" to use in Singapore
- As per mobile IP terminology, the home agent tunnells the packet to the COA.

The steps used in the operation of mobile IP are the following:

Step 1: The remote client sends a datagram to the MN using its home address. It reaches the home agent as usual.

Step 2: The home agent encapsulates that datagram in a new packet and sends it to the foreign agent.

Desirable Features of Mobile IP

Some of the features required of mobile IP are the followings.

Transparency: The IP address is to be managed transparently and there should not be any effect of mobility on any ongoing communication.

Compatibility: Mobile IP should be compatible with the existing Internet protocols.

Security: Mobile IP should, as far as possible, provide users with secure communications over the Internet.

Efficiency and Scalability: In the event of worldwide support, there can be a large number of mobile systems in the whole Internet. It should also be scalable to support billions of moving hosts worldwide.

3. Explain the operation of mobile IP with the help of a suitable schematic diagram and by using suitable examples.
Explain about the key mechanism in Mobile IP. (16) [Nov 2016]

Key Points

- Discovering the care-of-address
- Registering the care-of-address
- Tunnelling to the care-of-address

Key Mechanism in Mobile IP

Mobile IP is associated with the following three basic mechanisms:

- Discovering the care-of-address
- Registering the care-of-address
- Tunnelling to the care-of-address

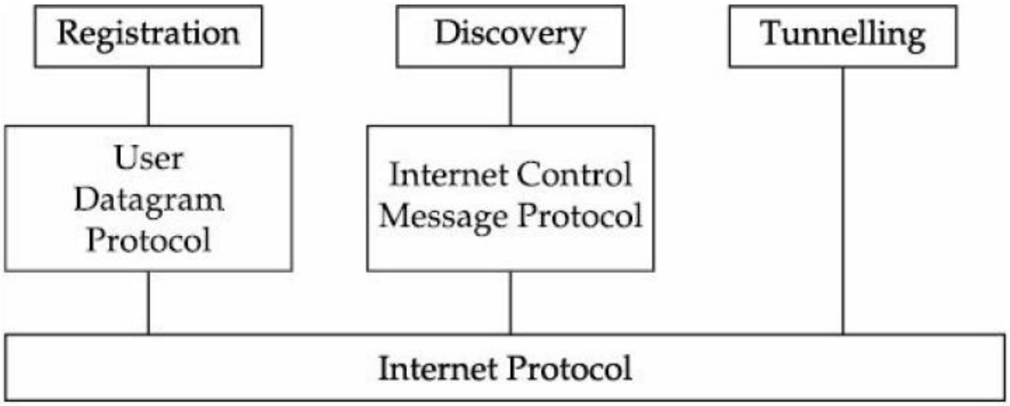


Figure 4.2 A schematic model of Mobile IP.

Discovering the care-of-address

Each mobile node uses a discovery protocol to identify the respective home and foreign agents.

The discovery of the care-of-address consists of four important steps.

1. Mobile agents advertise their presence by periodically broadcasting the **agent advertisement** messages.
2. The mobile node receiving the **agent advertisement** message observes whether the message is from its own home agent and determines whether it is on the home network or on a foreign network.
3. If a mobile node does not wish to wait for the periodic advertisement, it can send out **agent solicitation** messages that will be responded to by a mobility agent.
4. The process of agent advertisements, involves the following activities:
    - Foreign agents send messages to advertise the available care-of-addresses.
    - Home agents send advertisements to make themselves known.
    - Mobile hosts can issue agent solicitations to actively seek information.
    - If a mobile host has not heard from the foreign agent to which its current care-of-address belongs, it takes up another care-of-address.

Registering the care-of-address

- If a mobile node discovers that it is on the home network, it operates without requiring any mobility services.
- If a mobile node obtains a care-of-address from a foreign agent, then this address should be registered with the home agent.
- The mobile node sends a request for registration to its home agent along with the care-of-address information whenever the home agent receives the registration request information.
- The routing table is updated and it sends back the registration reply to the mobile node.
- The mobile node makes use of the registration procedure to intimate the care-of-address to a home agent.

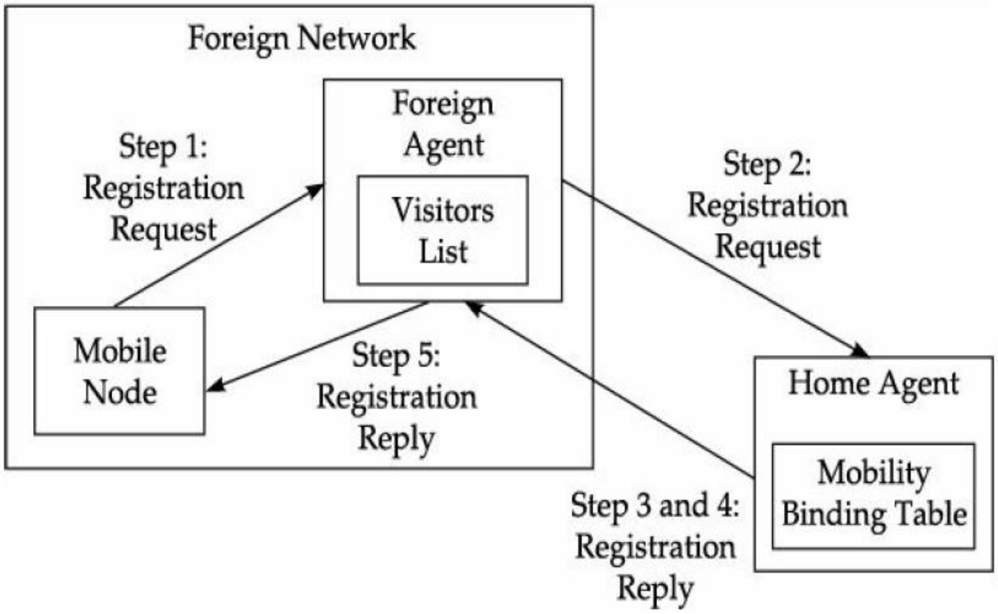

Foreign Network
Foreign Agent
Visitors List
Step 1: Registration Request
Step 2: Registration Request
Mobile Node
Step 5: Registration Reply
Home Agent
Mobility Binding Table
Step 3 and 4: Registration Reply

Figure 4.3 Registration process in Mobile IP.

The registration process consists of the following steps:

1. If the mobile node is on a new network, it registers with the foreign agent by sending a **registration request** message which includes the permanent IP address of the mobile host and the IP address of its home agent.
2. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.
3. When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of-address of the mobile node with its home address.
4. The home agent then sends an acknowledgement to the foreign agent.
5. The foreign agent in turn updates its visitors list by inserting the entry for the mobile node and relays the reply to the mobile node.

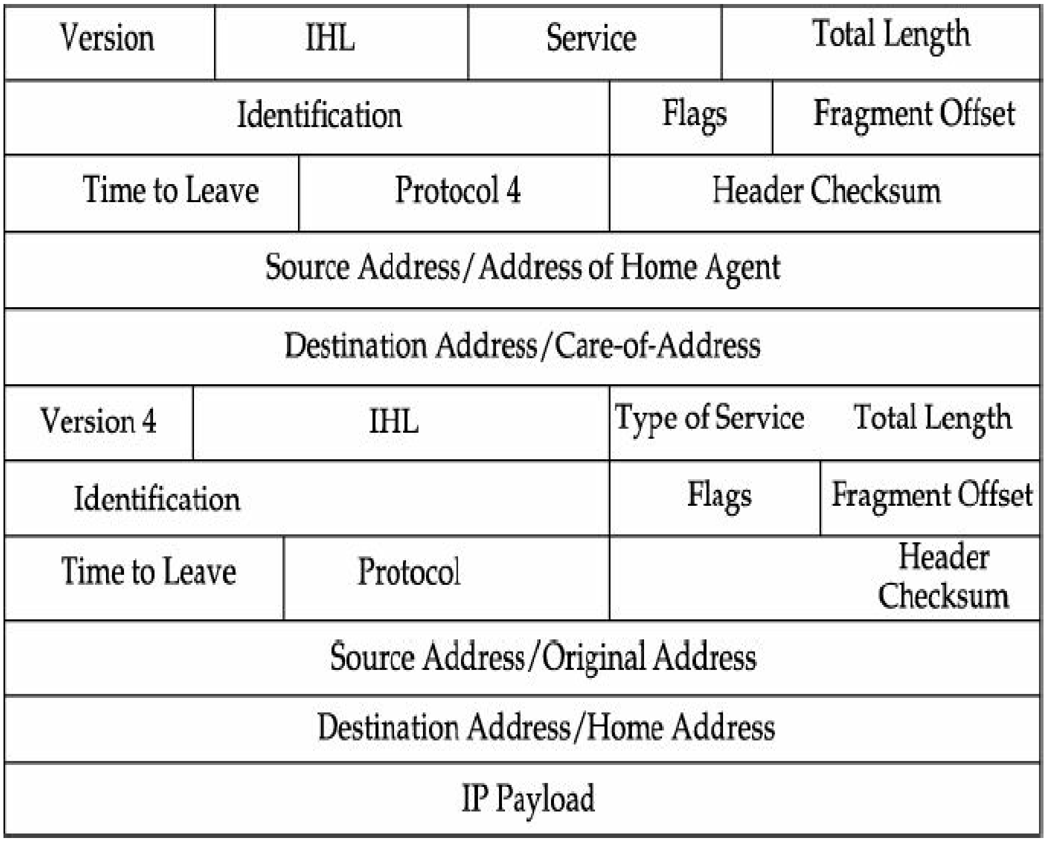
Box – Security in Mobile IP

Security is very important in Mobile IP as mobile nodes are often connected to the Internet via wireless links which are very vulnerable to security attacks.
For example, during the registration procedure the home agent should be convinced that it is getting the authentic registration request from a mobile node. Mobile IP solves this problem by specifying a security association between the home agent and the mobile node.

Tunnelling to the care-of-address

Tunnelling takes place to forward an IP datagram from the home agent to a care-of-address.
This involves carrying out the following steps:

- When a home agent receives a packet addressed to a mobile host, it forwards the packet to the care-of-address using IP-within-IP (encapsulation).
- Using IP-within-IP, the home agent inserts a new IP header in front of the IP header of any datagram.
- Destination address is set to the care-of-address.
- Source address is set to the home agent's address.
- After stripping out the first header, IP processes the packet again.



Version	IHL	Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol 4	Header Checksum	
Source Address/Address of Home Agent			
Destination Address/Care-of-Address			
Version 4	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Leave	Protocol		Header Checksum
Source Address/Original Address			
Destination Address/Home Address			
IP Payload			

Figure 4.4 IP encapsulation in mobile IP.

4. Discuss how optimization in achieved in mobile IP?

Key Points

- Route Optimization
- Binding request
- Binding acknowledgement
- Binding update
- Binding warning

Route Optimization

In the mobile IP protocol, all the data packets to the mobile node go through the home agent. Because of this there will be heavy traffic between HA and CN in the network, causing latency to increase.

Therefore, the following route optimization needs to be carried out to overcome this problem.

- Enable direct notification of the corresponding host
- Direct tunnelling from the corresponding host to the mobile host
- Binding cache maintained at the corresponding host

The mobile IP scheme needs to support the four messages shown in Table 4.1.

The association of the home address with a care-of-address is called **binding.**

TABLE 4.1 Messages Transmitted in Optimized Mobile IP

Message type	**Description**
Binding request	If a node wants to know the current location of a mobile node (MN), it sends a request to home agent (HA).
Binding acknowledgement	On request, the node will return an acknowledgement message after getting the binding update message.
Binding update	This is a message sent by HA to CN mentioning the correct location of MN. The message contains the fixed IP address of the mobile node and the care-of-address. The binding update can request for an acknowledgement.
Binding warning	If a node decapsulates a packet for a mobile node (MN), but it is not the current foreign agent (FA), then this node sends a binding warning to the home agent (HA) of the mobile node (MN).

5. Explain IP in IP, minimal IP and GRE encapsulation methods. (8) [May 2016]

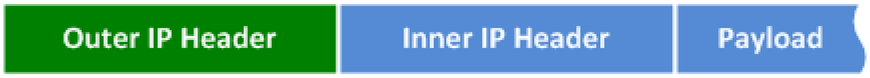
What is Encapsulation? Explain in detail the various encapsulation techniques in mobile IP. (16) [May 2017]

Encapsulation:

- Encapsulation describes the process of placing an IP datagram inside a network packet or frame.
- Encapsulation refers to how the network interface uses packet switching hardware

IPIP

- IP-in-IP encapsulation is exactly what it sounds like: one IP packet encapsulated inside another. The protocol field of the outer header is set to 4 for IPv4 or 41 for IPv6.

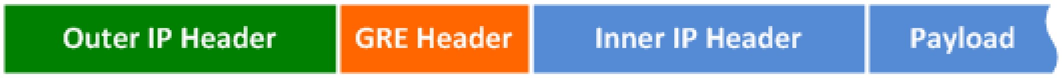


Minimal IP

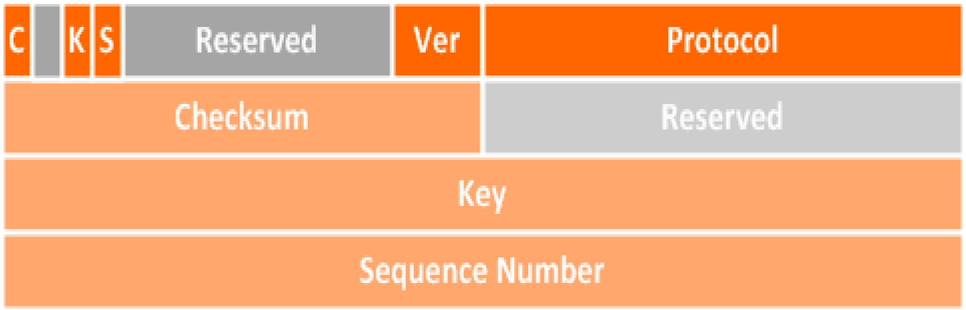
- A minimal forwarding header is defined for datagrams which are not fragmented prior to encapsulation. Use of this encapsulating method is optional.
- Minimal encapsulation MUST NOT be used when an original datagram is already fragmented, since there is no room in the minimal forwarding header to store fragmentation information.
- To encapsulate an IP datagram using minimal encapsulation, the minimal forwarding header is inserted into the datagram.

GRE

- Generic Routing Encapsulation (GRE) and IP-in-IP (IPIP) are two rather similar tunneling mechanisms which are often confused.
- GRE (defined in RFC 2784 and updated by RFC 2890) goes a step further than IP-in-IP, adding an additional header of its own between the inside and outside IP headers.



- The GRE header is variable in length, from 4 to 16 bytes, depending on which optional features have been enabled.



- C, K, and S: Bit flags which are set to one if the checksum, key, and sequence number fields are present, respectively
- Ver: GRE version number (zero)
- Protocol: Ethertype of the encapsulated protocol
- Checksum: Packet checksum (optional)
- Key: Tunnel key (optional)
- Sequence Number: GRE sequence number (optional)

Here's a sample capture of GRE in action. Note that GRE can theoretically encapsulate any layer three protocol with a valid Ether type, unlike IPIP, which can only encapsulate IP.
GRE can be encapsulated by either IPv4 or IPv6 on IOS. (The multipoint option is used for Dynamic Multipoint VPN (DMVPN).)

```
Router(config)# interface tun0
Router(config-if)# tunnel mode gre ?
  ip          over IP
  ipv6        over IPv6
  multipoint  over IP (multipoint)
```

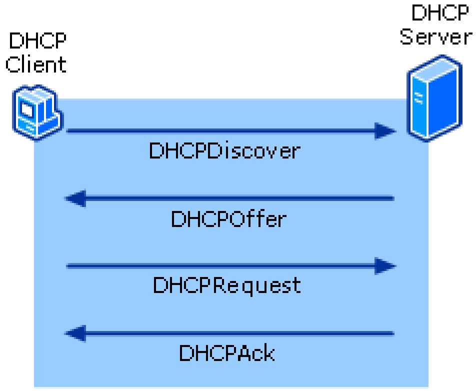
To summarize, GRE can:

- Encapsulate any layer three protocol (versus just IP)
- Add an additional checksum (which isn't useful for TCP/IPv4)
- Specify a tunnel key
- Enforce packet sequencing

6. With a diagram explain DHCP & its protocol architecture. (8) [Nov 2016]

DHCP Architecture

- The DHCP architecture consists of DHCP clients, DHCP servers, and DHCP relay agents on a network. The clients interact with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases.



Interactions between client and server

- DHCP servers and DHCP clients communicate through a series of DHCP messages. To obtain a lease, the DHCP client initiates a conversation with a DHCP server using a series of these DHCP messages.

DHCP messages

- The following list includes the eight types of messages that can be sent between DHCP clients and servers.

DHCPDiscover

- Broadcast by a DHCP client when it first attempts to connect to the network. The DHCPDiscover message requests IP address information from a DHCP server.

DHCPOffer

- Broadcast by each DHCP server that receives the client DHCPDiscover message and has an IP address configuration to offer to the client.
- The DHCPOffer message contains an unleased IP address and additional TCP/IP configuration information, such as the subnet mask and default gateway.
- More than one DHCP server can respond with a DHCPOffer message.
- The client accepts the best offer, which, for a Windows DHCP client, is the first DHCPOffer message that it receives.

DHCPRequest

- Broadcast by a DHCP client after it selects a DHCPOffer.
- The DHCPRequest message contains the IP address from the DHCPOffer that it selected. If the client is renewing or rebinding to a previous lease, this packet might be unicast directly to the server.

DHCPAck

- Broadcast by a DHCP server to a DHCP client acknowledging the DHCPRequest message.
- At this time, the server also forwards any options. Upon receipt of the DHCPAck, the client can use the leased IP address to participate in the TCP/IP network and complete its system startup.
- This message is typically broadcast, because the DHCP client does not officially have an IP address that it can use at this point.
- If the DHCPAck is in response to a DHCPInform, then the message is unicast directly to the host that sent the DHCPInform message.

DHCPNack

- Broadcast by a DHCP server to a DHCP client denying the client’s DHCPRequest message.
- This might occur if the requested address is incorrect because the client moved to a new subnet or because the DHCP client’s lease has expired and cannot be renewed.

DHCPDecline

- Broadcast by a DHCP client to a DHCP server, informing the server that the offered IP address is declined because it appears to be in use by another computer.

DHCPRelease

- ent by a DHCP client to a DHCP server, relinquishing an IP address and canceling the remaining lease. This is unicast to the server that provided the lease.

DHCPInform

- Sent from a DHCP client to a DHCP server, asking only for additional local configuration parameters; the client already has a configured IP address.
- This message type is also used by DHCP servers running Windows Server 2008 to detect unauthorized DHCP servers.

DHCP lease process

- A DHCP-enabled client obtains a lease for an IP address from a DHCP server.

- Before the lease expires, the DHCP client must renew the lease or obtain a new lease.
- Leases are retained in the DHCP server database for a period of time after expiration.
- By default, this grace period is four hours and cleanup occurs once an hour for a DHCP server running Windows Server 2008.
- This protects a client's lease in case the client and server are in different time zones, the internal clocks of the client and server computers are not synchronized, or the client is off the network when the lease expires.

7. What are the main functions of DHCP? Why is DHCP needed? Can it be used when nodes are mobile? Explain your answer. (Or) Explain the significance of Dynamic Host Configuration Protocol. Give examples of situations where it is useful.

Key Points

DHCP – Introduction

Benefits

- Reliable IP address configuration
- Reduced network administration

Why use DHCP - maintains a pool of IP addresses

Significance of Dynamic Host Configuration Protocol

DHCP supports three important mechanisms for IP address allocation

- Automatic allocation
- Dynamic allocation
- Manual allocation

Dynamic Host Configuration Protocol (DHCP)

- DHCP was developed based on bootstrap protocol (BOOTP). DHCP provides several types of information to a user including its IP address.
- To manage dynamic configuration information and dynamic IP addresses, IETF standardized an extension to BOOTP known as dynamic host configuration protocol (DHCP).
- The DHCP client and server work together to handle the roaming status and to assign IP address on a new network efficiently. The DHCP server allocates an IP address from a pool of IP addresses to a client.
- The BOOTP protocol is used for booting (starting) computers from the network. These are popularly used in case of diskless computers. Whenever a client requests an IP address from the server machine, BOOTP searches a table which matches to its physical address.

Benefits of DHCP

- **Reliable IP address configuration.** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

- **Reduced network administration.** DHCP includes the following features to reduce network administration:
  - Centralized and automated TCP/IP configuration.
  - The ability to define TCP/IP configurations from a central location.
  - The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
  - The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
  - The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP

- Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources.
- Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.
- DHCP enables this entire process to be automated and managed centrally. The **DHCP server maintains a pool of IP addresses** and leases an address to any DHCP-enabled client when it starts up on the network.
- Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.
- The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer.

The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.
- Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name. For a full list of DHCP options, see "DHCP Tools and Settings."

Significance of Dynamic Host Configuration Protocol

- DHCP is an extension to the BOOTP and compatible with it. For example, if a host is running BOOTP, it can also request configuration (example: static configuration) from a DHCP server node.

- The importance of DHCP in a mobile computing environment is that it provides temporary IP addresses whenever a host moves from one network to another network.

DHCP supports the following three important mechanisms for IP address allocation:

Automatic allocation: In automatic allocation, DHCP assigns a permanent IP address to a particular client.

Dynamic allocation: In dynamic allocation, DHCP assigns IP address to a client for a specific period of time.

Manual allocation: In manual allocation, a client's IP address is assigned by the network administrator, where the DHCP is used to inform the address assigned to clients.

Mobile Transport Layer

- In mobile computing applications, Transmission Control Protocol (TCP) is possibly the most popular transport layer protocol. In fact, TCP is the **de facto** standard transport layer protocol for applications that require guaranteed message delivery.
- TCP is a connection-oriented protocol. UDP (User Datagram Protocol), on the other hand, is a connectionless protocol in the TCP/IP protocol suite and does not guarantee reliable data delivery. However, when the traditional TCP is used in mobile computing networks, it operates in a highly inefficient and unsatisfactory manner.
- TCP needs several special adaptations to make it suitable for use in wireless networks.

8. Explain in detail about the basic concepts of Adhoc network.

Key Points

- Adhoc basic concepts – Schematic model of a mobile Adhoc Network
- Routing in a MANET

Adhoc Basics Concepts

How Is an Ad Hoc Network Set Up without the Infrastructure Support?

Adhoc network is defined as a set of mobile devices can communicate with each other in the **absence of** any form of fixed networking infrastructures such as **hubs, routers, base stations**, etc.

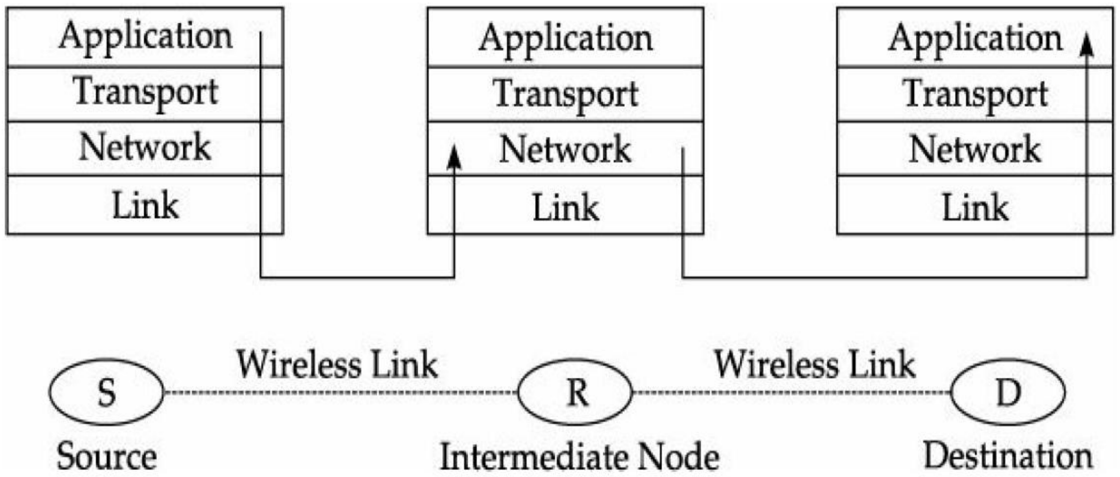


Figure 7.1 *A schematic model of a mobile ad hoc network.*

In this figure, suppose the mobile device S wants to communicate with the device D.

- Assume that S and D are not within the transmission range of each other and cannot directly communicate with each other.
- They can take the help of node R to relay packets from each other.
- R is primarily an independent device and not a networking infrastructure, yet R is acting as some sort of a router operating at the network (or Internet) layer to facilitate communication.

Routing in a MANET

- In a wired network, a router determines the path that needs to be followed by a packet based on the information contained within the IP address of the destination, and uses this information to forward a packet towards its destination.
- In an ad hoc network, such a simple and efficient routing protocol is difficult to deploy.
- In a MANET(Mobile Adhoc Network) the topology of the network and consequently the routes between different devices change dynamically as nodes move away or fail.
  Packet routing is a critical and complex issue in MANETs.

9. Explain in detail about characteristics of Mobile Adhoc Networks.
Explain characteristics, Applications of MANET. (4+4) [May 2016]

Key Points

- Lack of fixed infrastructure
- Dynamic topologies
- Bandwidth constrained, variable capacity links
- Energy constrained operation
- Increased vulnerability

Characteristics of Mobile Ad Hoc Networks (MANETs)

1. Lack of fixed infrastructure:

In the absence of any fixed networking infrastructure, a pair of nodes can either communicate directly when they are in the transmission range of each other, or they can communicate using a multi-hop communication that gets set up through several devices located between them.

2. Dynamic topologies:

Since the devices in a MANET are allowed to move arbitrarily, the network topology can change unpredictably. The rate of topology change depends on the speed of movement of the mobile devices. The speed of movement of a mobile device can vary greatly with the time of the day and the specific MANET application being considered.

3. Bandwidth constrained, variable capacity links:

Wireless links have significantly lower capacity than their wired counterparts. Further, factors such as fading, noise, and interference can change the available bandwidth of a wireless link arbitrarily with time. Consequently, the bandwidth of a link can change arbitrarily with time.

4. Energy constrained operation:

The nodes in a MANET rely on battery power. These batteries are small and can store very limited amounts of energy. On the other hand, transmissions and processing required during routing involve expenditure of substantial amount of energy causing the batteries to get rapidly drained out, unless the routing protocol is carefully designed. Therefore, energy conservation is usually considered to be an important objective of MANET routing protocols.

5. Increased vulnerability:

MANETs are prone to many new types of security threats that do not exist in the case of their wired counterparts. Many of these threats arise due to the underlying wireless transmissions and the deployment of collaborative routing techniques.

There are increased possibilities of eavesdropping, spoofing, denial-of-service attacks in these networks. It is very difficult to identify the attacker since the devices keep moving and do not have a global identifier.

Other characteristics:

Other distinguishing characteristics of a MANET include a distributed peer-to-peer mode of operation, multi-hop routing, and relatively frequent changes to the concentration of nodes over any specific area.

MANET Operational Constraints

The nodes in a MANET have low processing capabilities and these are connected by low bandwidth wireless links.

An appropriate routing protocol for a MANET should keep the computational and communicational overheads low, since the nodes in a MANET have low computational capability, storage capacity and battery power.

10. Explain in detail about the Applications of Adhoc networks.

Key Points

- Communication among portable computers
- Environmental monitoring
- Military
- Emergency applications

Applications

1. Communication among portable computers

- Miniaturization has allowed the development of many types of portables and computerized equipment, which have become very popular.
- Many of these portables work meaningfully when connected to some network, possibly a LAN or the Internet. For this, the portables are typically required to be within the range of some wireless hub.
- Satisfaction of this requirement would, however, drastically reduce the flexibility and the mobility of the devices.
- In this case, using MANET the audience can exchange notes, and also can surf the Web if at least one of the hand-held devices has access to Internet, for example, through a data card.
- If the mobile devices are present in sufficient density, network connections among them can be established seamlessly to form a MANET over which the nodes can communicate and carry out the network operations.

2. Environmental monitoring

- Continuous data collection from remote locations is considered important for several applications such as environmental management, security monitoring, road traffic monitoring and management, etc.
- Miniaturized sensors have proved to be an effective means of gathering environmental information such as rainfall, humidity, presence of certain animals, etc.
- In this environmental monitoring application, a large number of sensors nodes are deployed in the environment.
- Such ad hoc sensor networks can be deployed to collect data from remote locations and the sensor nodes can even respond to some commands issued by the data collection centre.
- MANETs efficiently handle the introduction of new sensors into an already operational sensor network as well as can handle dynamic disconnections of nodes.
- Since each sensor acts as a hub, the range over which the sensors can be spread is tremendously increased.

3. Military

- Ad hoc networking of this equipment can allow a military setup to take advantage of an information network among the soldiers, vehicles, and military information headquarters.
- For example, an ad hoc network can be automatically set up at a battlefront among the equipment, and the hand-held devices can collect information from and disseminate command to the frontline personnel.

4. Emergency applications

- Ad hoc networks do not require any pre-existing infrastructure.
- These networks, therefore, can be deployed easily and rapidly in emergency situations such as a search and rescue operation after a natural disaster, and for applications such as policing and fire fighting.

11. Explain in detail about MANET Design Issues.

Explain the design issues in MANET and the applications of adhoc network. (13) [Apr 2018]

Explain the design issues of MANET routing protocols in detail. (16)

[May 2017]

Key Points

- Network size and node density
- Connectivity
- Network topology
- User traffic
- Operational environment
- Energy constraint

MANET Design Issues

Network size and node density

- Network size and node density are the two important parameters of a MANET that need to be considered while designing an appropriate routing protocol for a network.
- Network size refers to the geographical coverage area of the network and network density refers to the number of nodes present per unit geographical area.
- For larger networks, clustering is essential to keep the communication overheads low.
- The cluster size as well as a specific clustering solution for a network would, to a large extent, depend on node density.

Connectivity

- The term connectivity of a node usually refers to the number of neighbours it has.
- Here a neighbor of a node is one that is in its transmission range.
- The term connectivity is also sometimes used to refer to a link between the two nodes.
- The term link capacity denotes the bandwidth of the link. In a MANET, both the number of neighbouring nodes and the capacities of the links to different neighbours may vary significantly.

Network topology

- The topology of a network denotes the connectivity among the various nodes of the network. Mobility of the nodes affects the network topology.
- Due to node mobility, new links can form and some links may get dissolved. Other than mobility, nodes can become inoperative due to discharged batteries or hardware failures, and thereby cause changes to the topology.
- The rate at which the topology changes needs to be appropriately considered in the design of an effective network.

User traffic

- The design of a MANET is carried out primarily based on the anticipated node density, average rate of node movements, and the expected traffic.
- The traffic in a network can be of various types.
- A network protocol should leverage the characteristics of specific traffic types that are expected to improve its performance.

The common traffic types are the following:

- Bursty traffic

- Large packets sent periodically
- Combination of the above two types of traffic

Operational environment

- The operational environment of a mobile network is usually either urban, rural and maritime. These operational environments support the Line of Sight (LOS) communication.
- But, there can be a significant difference in the node density and mobility values in different operational environments, requiring different designs of mobile networks to suit an operational environment.

Energy constraint

- No fixed infrastructure exists in a MANET; the mobile nodes themselves store and forward packets. This additional role of mobile nodes as routers leads to nodes incurring perennial routing-related workload and this consequently results in continual battery drainage.
- Though this overhead is indispensable if the network is to be kept operational, the energy spent can be substantially reduced by allowing the nodes to go into a sleep mode whenever possible.

12. Explain in detail about popular MANET routing protocols and Proactive protocol-DSDV, Reactive Routing Protocols – DSR, AODV, Hybrid routing –ZRP, Multicast Routing- ODMRP.

Keypoints

1. Destination-Sequenced Distance-Vector Routing Protocol (DSDV) - table-driven (Proactive Protocol) approach
2. Dynamic Source Routing (DSR) Protocol - on-demand (or Reactive Routing Protocol) routing protocol.
   - Route Cache
   - Route discovery
   - Route maintenance
3. Ad Hoc On-demand Distance Vector (AODV)- on-demand (or Reactive Routing Protocol) routing protocol
   - Route Request
   - Route Reply
4. Zone Routing Protocol (ZRP) - both on-demand and proactive (Hybrid) routing protocol
5. Multicast Routing Protocols for MANET - delivery of a message to a group of destination nodes in a single transmission

Popular MANET Routing Protocols

- Destination-Sequenced Distance-Vector Routing Protocol(DSDV)
- Dynamic Source Routing (DSR) Protocol
- Ad Hoc On-demand Distance Vector (AODV)
- Zone Routing Protocol(ZRP)
- Multicast Routing Protocols for MANET

a) Destination-Sequenced Distance-Vector Routing Protocol(DSDV)

- Destination-Sequenced Distance-Vector Routing (DSDV) is an important MANET routing protocol. It is based on the table-driven (proactive) approach to packet routing.
- In DSDV, each node in a MANET maintains a routing table in which all of the possible destinations and the number of hops to each destination are recorded.
- Each node maintains information regarding routes to all the known destinations. The routing information is updated periodically.
- Also, there is traffic overhead even if there is no change in network topology. Nodes maintain routes which they may never use.
- A sequenced numbering system is used to allow mobile nodes to distinguish stale routes from new ones. Updated routing tables are exchanged periodically among the nodes of the network to maintain table consistency.
- DSDV uses two types of route update packets. The first is known as *full dump*. This type of packet carries all the available routing information and can require multiple network protocol data units (NPDUs) to be transmitted.
- The mobile nodes maintain an additional table where they store the data received through the incremental routing information packets from various nodes.

Important steps in the operation of DSDV

1. Each router (node) in the network collects route information from all its neighbours.
2. After gathering information, the node determines the shortest path to the destination based on the gathered information.
3. Based on the gathered information, a new routing table is generated.
4. The router broadcasts this table to its neighbours. On receipt by neighbours, the neighbor nodes recompute their respective routing tables.
5. This process continues till the routing information becomes stable.

Figure 7.3 shows an example of a MANET. Table 7.1 is the routing table of the node N 4 at the moment before the movement of nodes. The metric field in the routing table helps to determine the number of hops required for a packet to traverse to its destination.

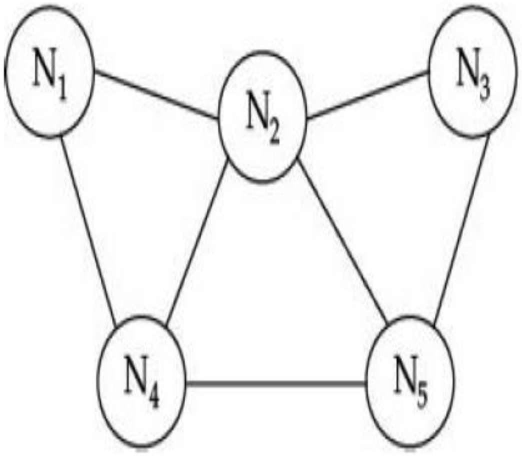
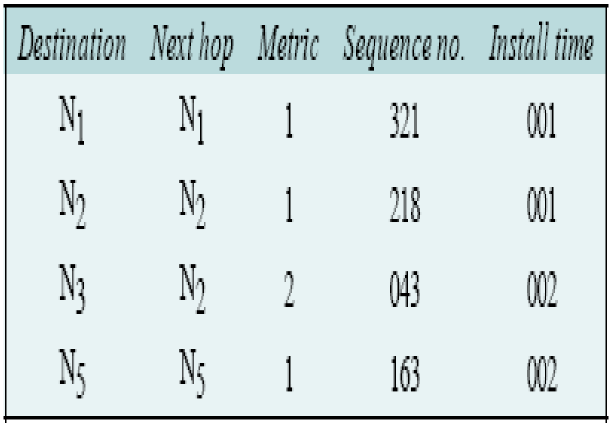


Figure 7.3 *An example of a MANET topology at a given instant of time.*

TABLE 7.1 DSDV Routing Table for the MANET of Figure 7.3 at Node N_4



Destination	Next hop	Metric	Sequence no.	Install time
N_1	N_1	1	321	001
N_2	N_2	1	218	001
N_3	N_2	2	043	002
N_5	N_5	1	163	002

2. Dynamic Source Routing (DSR) Protocol

- Dynamic Source Routing (DSR) protocol was developed to be suitable for use in a MANET having a reasonably small diameter of about 5 to 10 hops and when the nodes do not move very fast.
- DSR is a source initiated on-demand (or reactive) routing protocol for ad hoc networks.
- It uses source routing, a technique in which the sender of a packet determines the complete sequence of nodes through which a packet has to travel.
- The sender of the packet then explicitly records this list of all nodes in the packet's header. This makes it easy for each node in the path to identify the next node to which it should transmit the packet for routing the packet to its destination.
- In this protocol, the nodes do not need to exchange the routing table information periodically, which helps to reduce the bandwidth overhead associated with the protocol.
- Each mobile node participating in the protocol maintains a *routing cache* which contains the list of all routes that the node has *learnt*.
- Whenever a node finds a new route, it adds the new route to its *routing cache*. Each mobile node also maintains a sequence counter called *request id* to uniquely identify the last request it had generated.
- The pair < source address, request id > uniquely identifies any request in the ad hoc network.

Illustrate DSR routing in detail and compare it with DSDV. (13) [Nov 2018]

Explain DSR Routing Protocols in detail. (8) [May 2016]

Discuss Route Discovery and Route Maintenance mechanisms in DSR with illustrations. List its merits and demerits. (16) [Nov 2017]

DSR works in two phases:

(i) Route discovery and
(ii)Route maintenance.

Route discovery

- Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network.
- When a node has a data packet to send, it first checks its own routing cache.
- If it finds a valid route in its own routing cache, it sends out the packet using this route.
- Otherwise, it initiates a route discovery process by broadcasting a route request packet to all its neighbours.
- The route request packet contains the source address, the request id and a route record in which the sequence of hops traversed by the request packet, before reaching the destination is recorded.

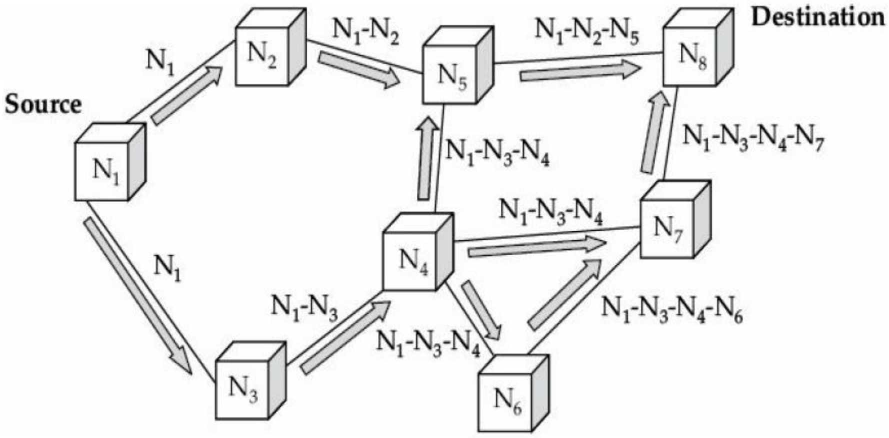


Figure 7.4 *An example of the route discovery process in DSR.*

- Suppose a node N1 wishes to send a message to the destination node N8. The intermediate nodes are N2, N3, N4, N5, N6, N7.
- The node N1 initiates the route discovery process by broadcasting a *route request* packet to its neighbours N2 and N3.
- Note that each node can have multiple copies of the route request packet arriving at it.
- The propagation of route reply is shown in Figure 7.5, and the acknowledgement messages from destination to source are indicated by thick arrows.

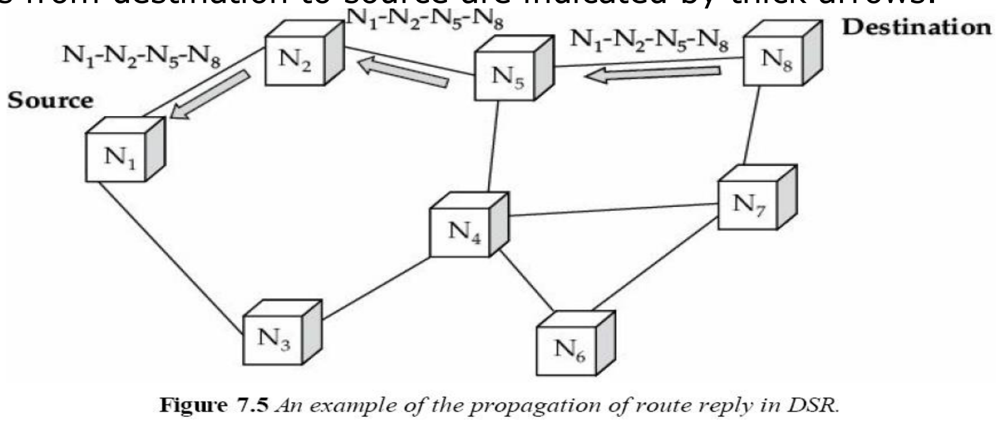


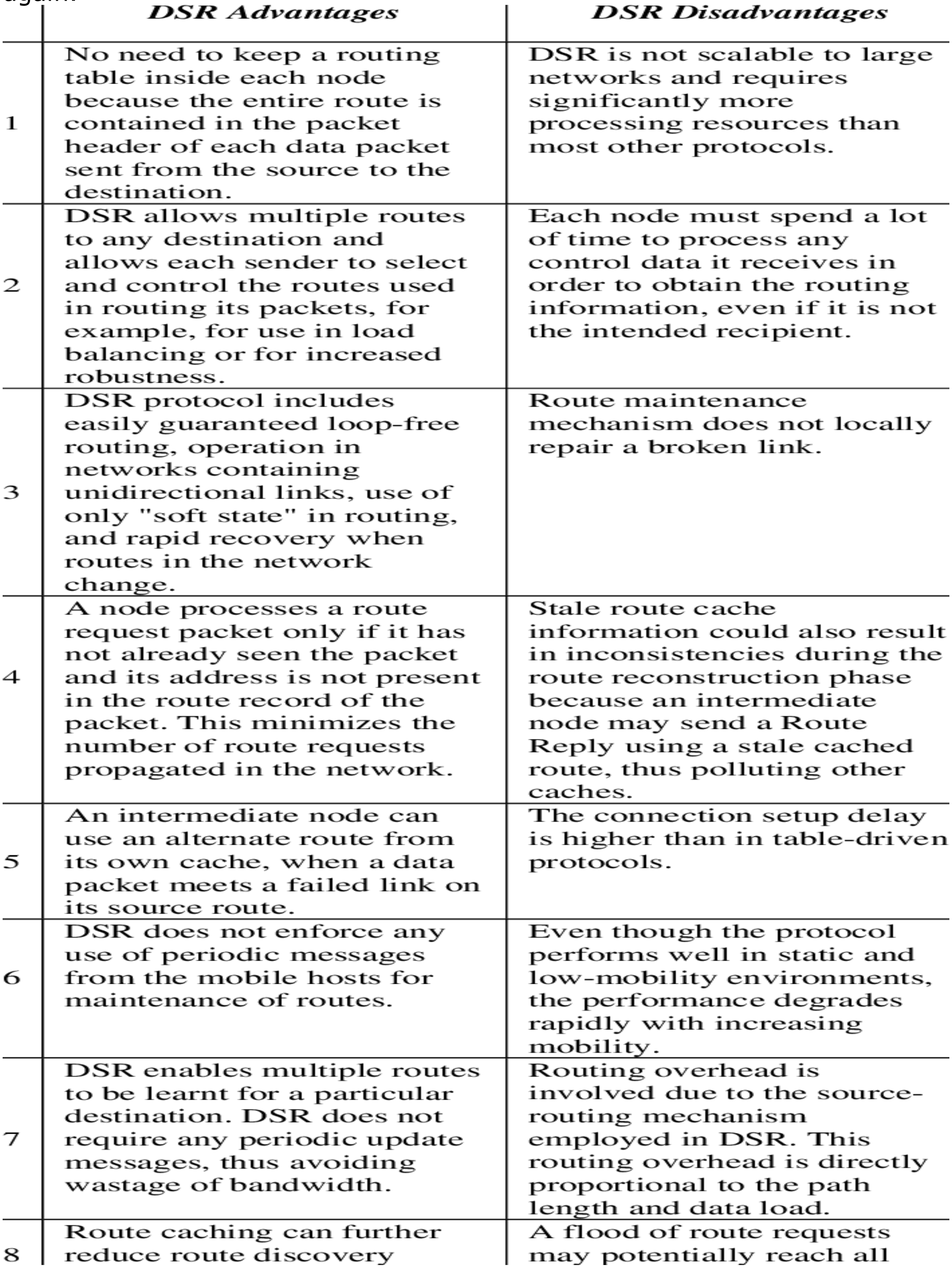
Figure 7.5 *An example of the propagation of route reply in DSR.*

Route maintenance

- Route maintenance is the process of monitoring the correct operation of a route in use and taking any corrective action when needed.
- When a host (source) while using a route, finds that it is inoperative, it carries out route maintenance.

- Whenever a node wanting to send a message finds that the route is broken, it would help if it already knows of some alternative routes.
- If it has another route to the destination, it starts to retransmit the packet using the alternative route. Otherwise, it initiates the route discovery process

again.



	DSR Advantages	*DSR Disadvantages*
1	No need to keep a routing table inside each node because the entire route is contained in the packet header of each data packet sent from the source to the destination.	DSR is not scalable to large networks and requires significantly more processing resources than most other protocols.
2	DSR allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness.	Each node must spend a lot of time to process any control data it receives in order to obtain the routing information, even if it is not the intended recipient.
3	DSR protocol includes easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and rapid recovery when routes in the network change.	Route maintenance mechanism does not locally repair a broken link.
4	A node processes a route request packet only if it has not already seen the packet and its address is not present in the route record of the packet. This minimizes the number of route requests propagated in the network.	Stale route cache information could also result in inconsistencies during the route reconstruction phase because an intermediate node may send a Route Reply using a stale cached route, thus polluting other caches.
5	An intermediate node can use an alternate route from its own cache, when a data packet meets a failed link on its source route.	The connection setup delay is higher than in table-driven protocols.
6	DSR does not enforce any use of periodic messages from the mobile hosts for maintenance of routes.	Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
7	DSR enables multiple routes to be learnt for a particular destination. DSR does not require any periodic update messages, thus avoiding wastage of bandwidth.	Routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length and data load.
8	Route caching can further reduce route discovery	A flood of route requests may potentially reach all

3. Ad Hoc On-demand Distance Vector (AODV)

- The route discovery and route maintenance activities in AODV are very similar to those for the DSR protocol.

- AODV does make use of hop-by-hop routing, sequence numbers and beacons.
- The node that needs a route to a specific destination generates a *route request*.
- The *route request* is forwarded by intermediate nodes which also learn a reverse route from the source to themselves.
- When the request reaches a node with route to destination, it generates a *route reply* containing the number of hops required to reach the destination.
- All nodes that participate in forwarding this reply to the source node create a forward route to destination.
- This route created from each node from source to destination is a hop-by-hop route.

Recollect that DSR includes the complete route in packet headers.

- The large headers can substantially degrade the performance, especially when the data content of packets is small.
- AODV attempts to improve upon DSR by maintaining routing tables at the nodes, so that the data packets do not have to contain the routes.
- AODV retains a positive feature of DSR, in that the routes are maintained only between those nodes that need to communicate.
- If a link break occurs while a route is being used to transmit a message, a route error message is sent to the source node by the node that observes that the next link in the route has failed.

4. Zone Routing Protocol

- The Zone Routing Protocol (ZRP) is a hybrid protocol. It incorporates the merits of both on-demand and proactive routing protocols.
- A routing zone comprises a few MANET nodes within a few hops from the central zone. Within a zone, a table-driven routing protocol is used.
- If a destination node happens to be outside the source's zone, ZRP employs an ondemand route discovery procedure which works as follows.
- The source node sends a route request to the border nodes of its zone, containing its own address, the destination address and a unique sequence number.
- Border nodes are those nodes which are some predefined number of hops away from the source. Each border node checks its local zone for the destination.

What Multicast routing protocols. (8) [Nov 2016]

5.Multicast Routing Protocols for MANET

Multicast is the delivery of a message to a group of destination nodes in a single transmission as shown in Figure 7.6.

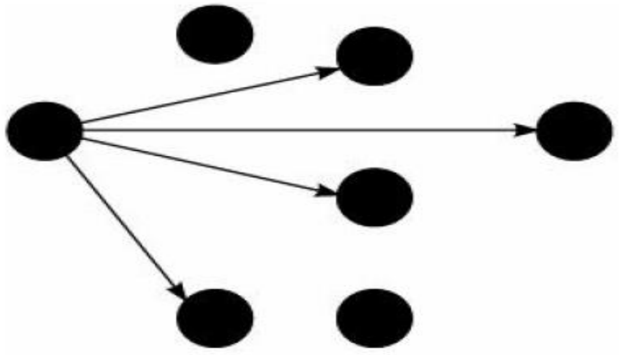


Figure 7.6 *Multicast transmission.*

For efficient operation of a multicast routing protocol, it is necessary to minimize the unnecessary packet transmissions as well as minimize the energy consumption.
In order to achieve this, a multicast transmission should not be approximated by multiple unicast transmissions.
<u>The popular MANET multicasting protocols are either tree-based or mesh-based:</u>

Tree-based protocol

Tree-based schemes establish a single path between any two nodes in the multicast group. These schemes require minimum number of copies per packet to be sent along the branches of the tree. Hence, they are bandwidth efficient.

Mesh-based protocol

Mesh-based schemes establish a mesh of paths that connect the sources and destinations. They are more resilient to link failures as well as to mobility.
The major disadvantage of this scheme is that multiple copies of the same packet are disseminated through the mesh, resulting in reduced packet delivery and increased control overhead under highly mobile conditions.

13. What are reactive and proactive protocols? Specify its advantages and Disadvantages. (8) [Nov 2016]

A Classification of Unicast MANET Routing Protocols

- Unicast routing protocols in MANETs are classified into proactive (table-driven), reactive (ondemand) and hybrid protocols.
- This classification is based on how a protocol manages to determine the route correctly in the presence of topology changes.

Proactive protocol:

- A proactive routing protocol is also known as a *table-driven* routing protocol.
- Each node in a *routing table maintains information about routes* to every other node in the network.
- These tables are *periodically updated* in the face of random network topology changes.
- Example protocol - Destination Sequenced Distance Vector (DSDV) protocol.

Reactive protocol:

- A reactive routing protocol is also known as an on-demand routing protocol, since in this protocol nodes do not *maintain up-to-date routes* to different destinations, and new routes are discovered only when required.
- When a node does not have knowledge about any route to a specific destination, it uses a flooding technique to determine the route.
- Two examples of on-demand routing protocols are:

(i) Dynamic source routing (DSR)
(ii) Ad hoc on-demand distance vector routing (AODV)

Hybrid routing protocols:

- Hybrid routing protocols have the characteristics of both proactive and reactive protocols. These protocols combine the good features of both the protocols.
- The hybrid routing protocols are designed to achieve increased scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.
- This is mostly achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes only when required using a route discovery strategy.
- Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of routing zones by each node.
- Example: Zone Routing Protocol (ZRP).

14. Explain in detail about Vehicular Adhoc Network. (VANET)

Key Points

- VANET – Introduction
- Uses

Vehicular Ad Hoc Networks (VANETs)

- A Vehicular Ad Hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network.
- VANETs were initially introduced for vehicles of police, fire brigades, and ambulances for safe travelling on road.
- In this network, a vehicle communicates with other vehicles that are within a range of about 100 to 300 metres. Multi-hop communication often results in rather large networks.
- In a city or a busy highway, the diameter of the network can be several tens of kilometres.
- Any vehicle that goes out of the signal range of all other vehicles in the network is excluded from the network.
- A vehicle that was outside the communication range of all other vehicles of a VANET can come in the range of a vehicle that is already in the network and as a result can join the network.
- A VANET can offer a significant utility value to a motorist.

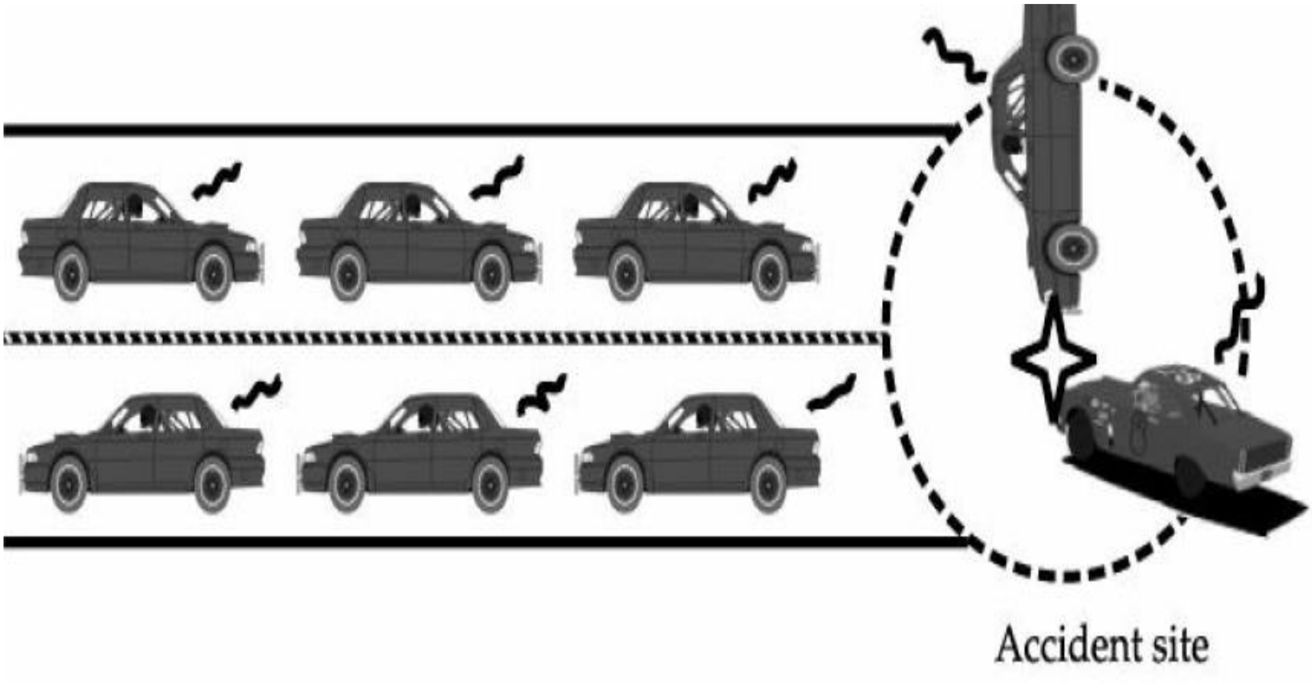


Figure 7.7 *A VANET use scenario.*

A few important uses of a VANET:

A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.

For example two vehicles are involved in a collision in the fig.

- The trailing vehicles get advance notification of the collision ahead on the road.
- The driver can also get advance information on the road condition ahead, or a warning about the application of emergency electronic brake by a vehicle ahead in the lane.
- A VANET can help disseminate geographical information to the driver as he continues to drive. For example, the driver would be notified of the nearby food malls or petrol refilling stations, map display, etc.
- Drivers may have the opportunity to engage in other leisurely tasks, such as VoIP with family, watch news highlights, listen to series of media files known as podcasts, or even carry out some business activities such as participate in an office video conference session.

15.Describe the architecture of VANET with the functionality of the components. Compare VANET vs MANET. (16) [Nov 2017]

Describe the architecture of VANET with a neat diagram. (13) [Apr 2018]

Draw and explain the architecture of VANET. (8) [May 2016]

The system architecture of vehicular ad hoc networks

Main Components

- The mobile domain consists of two parts:
  - Vehicle domain
  - Mobile device domain
- The vehicle domain comprises all kinds of vehicles such as cars and buses.

- The mobile device domain comprises all kinds of portable devices like personal navigation devices and smart phones.
- Within the infrastructure domain, there are two domains:
  - Roadside infrastructure domain
  - Central infrastructure domain
- The roadside infrastructure domain contains roadside unit entities like traffic lights.
- The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers.

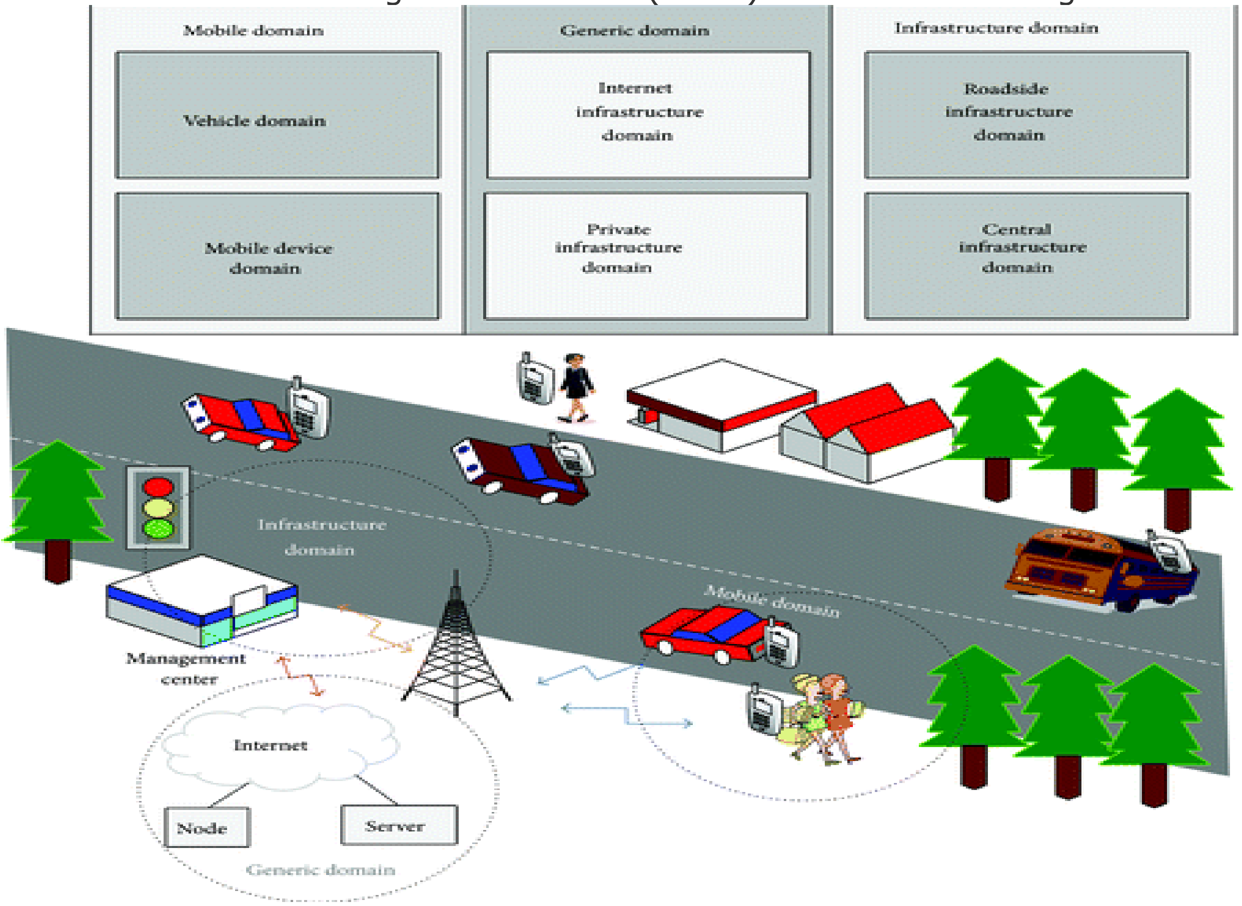
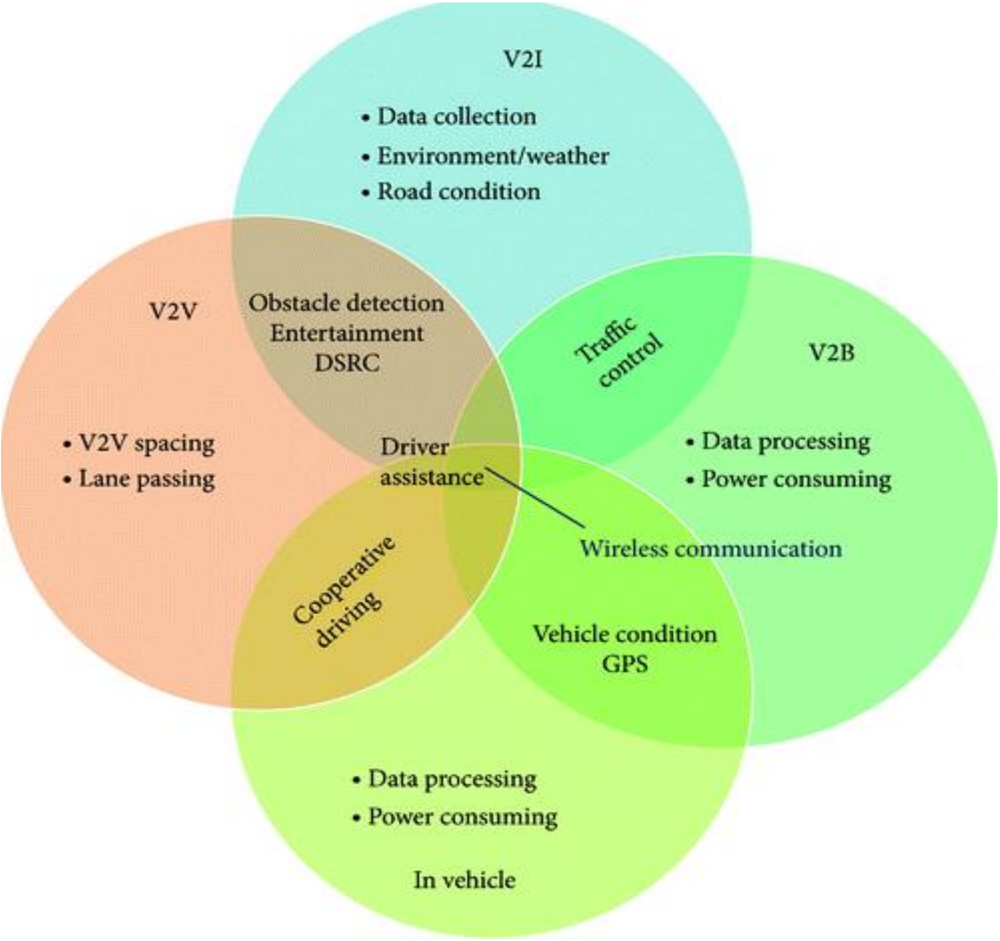


Figure 1 VANETs system domains.

- However, the development of VANETs architecture varies from region to region.
- In the CAR-2-X communication system which is pursued by the CAR-2-CAR communication consortium, the reference architecture is a little different.
- CAR-2-CAR communication consortium (C2C-CC) is the major driving force for vehicular communication in Europe and published its “manifesto” in 2007.
- This system architecture comprises three domains:
  - In-vehicle domain
  - Ad hoc domain
  - Infrastructure domain

Communication Architecture

Communication types in VANETs can be categorized into four types.



Key functions of each communication type.

In-vehicle communication

- Which is more and more necessary and important in VANETs research, refers to the in-vehicle domain.
- In-vehicle communication system can detect a vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.

Vehicle-to-vehicle (V2V)

- *Communication* can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-road infrastructure (V2I) communication

- It is another useful research field in VANETs.
- V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

Vehicle-to-broadband cloud (V2B) communication

- It means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G.
- As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

MANET Vs VANET

- A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.
- Consider a VANET to be a special category of MANET.
- The nodes are mobile in VANETs as well as in MANETs. However, the VANET nodes (vehicles) can communicate with certain roadside infrastructures or base stations.
- Further, the node mobility in a VANET is constrained to the road topologies, whereas the movement of nodes in a MANET is more random in nature.
- Considering that vehicles move over large distances at relatively high speeds, a VANET undergoes fast topological changes.
- Another important difference is that in a MANET, power is a major constraint but in VANET the battery power available in a vehicle is quite adequate.
- The issues such as the relatively larger size of VANETs compared to MANETs and the relatively high speed with which vehicles move, need to be appropriately considered for the design of an effective VANET.

16. Explain any two VANET routing protocol with an example. (16) [May 17]

Key Points

- Unicast routing protocols
- Multicast/Geocast Routing Protocols

1. Unicast routing protocols

- Unicast routing protocols transmit data packets from a single source to a single destination.
- They are primarily required to support personalised comfort applications and commercial applications such as internet connectivity and multimedia access.
- Unicast routing protocols are the most fundamental protocols in ad hoc environment and they form the basis for constructing other types of protocols.
- Unicast routing protocols are further classified into topology based, position based, cluster based and hybrid protocols

a) Topology based Routing Protocols

- Topology based protocols utilise the global information about the network topology and the information about the communication links for making routing decisions.
- These protocols use either proactive or reactive approaches for routing. Proactive approaches maintain the topology information about all the nodes irrespective of the fact that whether they are presently participating in the communication or not.
- These methods discover network topology information through periodic control packets and operate independent of current communication needs and network conditions.
- This increases overhead of joining new nodes into the network and consumes the network resources for control messages.
- Whereas, reactive protocols determine the routing information for a destination on-demand, only when it is needed for current communication.

- Reactive routing can be classified either as source routing or hop-by-hop routing.
- In source routing complete route information from source to destination is included in data packets, whereas in hop-by-hop routing only the next hop address and the destination address are provided.
- Hop-by-hop routing is better in terms of overall packet delivery ratio and end-to-end delay than source routing and hence it is adopted by most of the routing protocols.
- Examples of proactive protocols are Fisheye State Routing (FSR), Destination-Sequenced Distance-Vector (DSDV) and Optimized Link State Routing (OLSR).
- These protocols maintain a next hop table, which is exchanged among the neighbours.
- Reactive protocols such as Ad hoc On Demand distance Vector (AODV) and Dynamic Source Routing (DSR) have been considered efficient for multi-hop wireless ad hoc networks.
- AODV is a reactive routing protocol, which supports both unicast and multicast routing.
- It uses a destination sequence number, which makes it different from other on-demand routing protocols.
- It reduces memory requirements and the route redundancy. AODV responds to the link failure in the network.

b) Position based Routing Protocols

- In position based protocols, the routing decisions are based on geographic position of the vehicles.
- This does not require establishment or maintenance of routes, but requires location services to determine the position of the destination.
- Some of the commonly used location services include Global Position System (GPS), DREAM Location Services (DLS), Reactive Location Services (RLS) and Simple Location Services (SLS).
- With the advancement of GPS based location services, position based routing protocols are gaining importance. In position based protocols, the packet is sent without any knowledge of digital map to the one-hop neighbour, which is the closest to the position of the destination.
- Every node continuously sends beacon packets with their position information and other node identification parameters.
- Position based protocols are suitable for VANETs since they offer higher delivery ratio than topology based routing protocols in a highly mobile environment.
- They provide minimum delay in establishing the route and achieve good scalability. However, privacy is compromised since navigation information is disclosed on the network.

c) Non-Delay Tolerant Network (Non-DTN)

- Non-DTN protocols are also referred as Mindelay protocols and they aim at minimising the delivery time of the packets from source to destination.

- These protocols are suitable for time critical safety applications, which demand real-time response during data dissemination.
- The delay time in the transmission is the major concern in the design of Non-DTN protocols and usually the shortest path method is adopted.
- However, the shortest path may not always ensure faster delivery, especially when the traffic condition is sparse.
- These protocols are further classified into beacon based, nonbeacon based and hybrid routing protocols.

d) Delay Tolerant Network (DTN) Delay

- Tolerant Network is an approach to networking, which addresses the technical issues related to heterogeneous network that lack continuous network connectivity.
- They are characterized by limitations of latency, bandwidth, error probability and/or path stability.
- DTN uses carry and forward strategy to overcome frequent disconnection of nodes in the network. When a node cannot contact other nodes it stores the packet information and forwards the same when an opportunity arises.

2. Multicast/Geocast Routing Protocols

- Multicast routing enables dissemination of messages from single source to a group of destination nodes of interest.
- Geocast routing is basically a location based multicast routing, which aims to deliver information from a source node to all other nodes within a specified geographical region called a Zone of Relevance (ZOR).
- A Zone of Forwarding (ZOF) is defined within which the packets are directed instead of simply flooding the packets everywhere in the network.
- This reduces the overhead and network congestion. This protocol is applicable for safety and convenience related applications.

a) Topology based Approaches

- Topology based approaches select forwarding nodes based on the network topology information, which can be either multicast tree or multicast mesh.
- A multicast group is not constrained by a particular location; a group of members can be defined by unique and logical group identification such as class-D IP address.
- Robust Vehicular Routing (ROVER) [89] is a reliable geographical multicast protocol, where only control packets are broadcasted in the network and the data packets are unicasted.
- The objective of the protocol is to send a message to all other vehicles within a specified ZOR. When a vehicle receives a message, it accepts the message if it is within the ZOR.
- It also defines a ZOF, which includes the source and the ZOR.
- All vehicles in the ZOF are used in the routing process.
- It uses a reactive route discovery process within a ZOR.
- This protocol creates lot of redundant messages in the network, which leads to congestion and delay in data transfer.

b) Location based Approaches

- Location based approaches select forwarding nodes based on location information such as the position of sending/receiving nodes, the position of neighbouring nodes, and the coordinates of a multicast region.
- Since forwarding nodes are selected during dissemination of each multicast packet, there is no need to maintain multicast trees and hence less overhead.
- These protocols are further divided into two schemes:
- approaches with location-independent and approaches with location-dependent.
- Inter-Vehicles Geocast protocol (IVG) is developed for disseminating safety messages to vehicles on highways.
- The multicast group is defined dynamically using vehicles within the risk area, which is determined by the driving direction and position of vehicles.
- This group is defined temporarily and dynamically by the location, speed, and driving direction of vehicles.
- This protocol uses a timer based mechanism for forwarding messages and periodic broadcasts are used to overcome network fragmentation for delivering messages to the multicast members.
- The rebroadcast period is calculated based on the maximum speed of vehicles.
- Besides, IVG protocol reduces the number of hops by using the deferring time.
- A vehicle, which is farthest from the source node, has less deferring time to rebroadcast.

17. Explain the various security and attacks on VANET. (8) [May 2016]
Explain the architecture of VANET and various security attacks on VANET. (13) [Nov 2018]

Architecture
Refer Q.No.15

- VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives.

VANET Security Requirements

- Confidentiality,
- Integrity,
- Availability.
- Privacy
- Traceability and revocability
- Non-repudiation
- Real-time constraints
- Low Overhead

ATTACKS AND COUNTERMESURES IN VANETS

Denial of Service Attack:

- It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user.

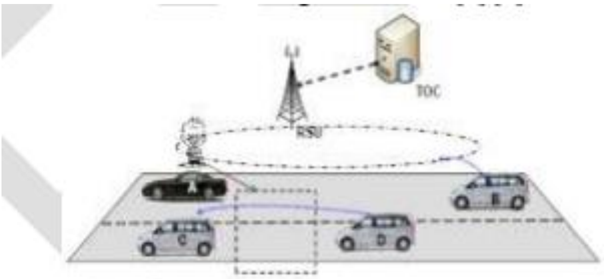


Fig. 2- Denial of Service Attack between V2V and V21

Fig. shows the whole scenario when the attacker A launches DOS attack in vehicular network as a result it Jams the whole communication medium between V2V and V2I and the authentic users (B, C, and D) cannot communicate with each other.

Distributed Denial of Service Attack (DDOS Attack):

- DDOS attacks are those attacks in which attacker attacks in distributed manner from different locations. Attacker may use different timeslots for sending the messages.
- Nature and time slot of the message can be varied from vehicle to vehicle of the attackers. The aim of attacker is same as DOS attack

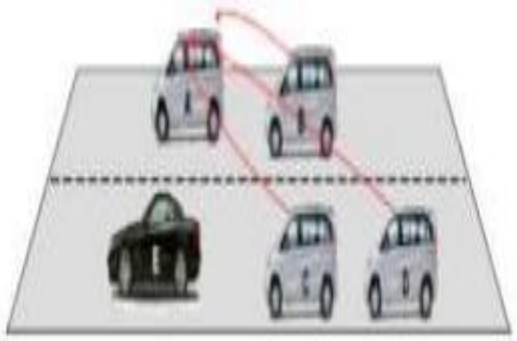


Fig. 3- DDOS Attack in vehicle to vehicle communication

Fig. explains the vehicle to vehicle (V2V) DDOS attack scenario in which attackers (B,C,D) launches DDOS on vehicle A.

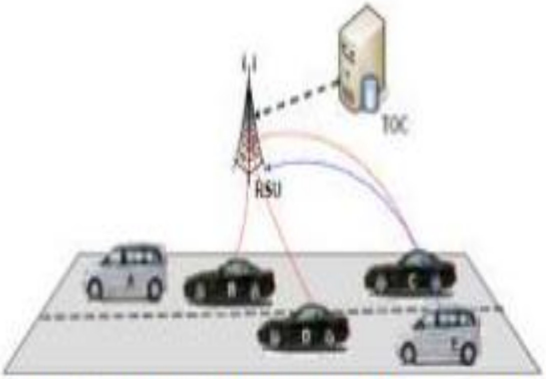


Fig. 4- DDOS Attack in vehicle to Infrastructure communication

Fig explains DDOS attack in vehicle to infrastructure communication. Here B,C,D are the attackers which attacks the infrastructure from different locations.
Whereas other vehicles (A,E) in the network want to access the network then the infrastructure is overloaded.

Sybil Attack:

- It is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity.
- It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route.
- The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route.

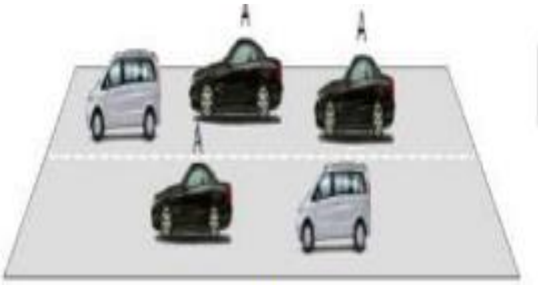


Fig. 5- Sybil Attack

Timing Attack:

- The main objective of attacker is to add some time slot in the original message that creates delay in the original message and these messages are received after these requires a time.
- AS we know safety applications are time critical applications if delay occurs in these applications then major objective of these applications is also finished.

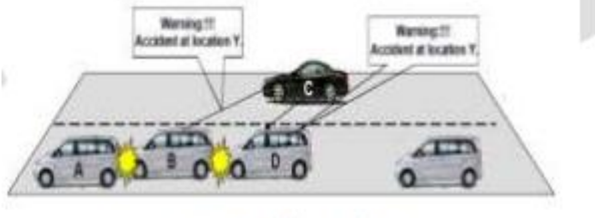


Fig. 9- Timing Attack

Fig. shows the complete scenario of the timing attack in which vehicle C is attacker which receives warning message from other vehicle B and then pass this message to other vehicle D by adding some time. Whenever the other D receives this message then accident actually occurs.

18. Explain in detail about MANET Vs VANET.

- A MANET is a collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.
- Consider a VANET to be a special category of MANET.
- The nodes are mobile in VANETs as well as in MANETs. However, the VANET nodes (vehicles) can communicate with certain roadside infrastructures or base stations.
- Further, the node mobility in a VANET is constrained to the road topologies, whereas the movement of nodes in a MANET is more random in nature.
- Considering that vehicles move over large distances at relatively high speeds, a VANET undergoes fast topological changes.
- Another important difference is that in a MANET, power is a major constraint but in VANET the battery power available in a vehicle is quite adequate.
- The issues such as the relatively larger size of VANETs compared to MANETs and the relatively high speed with which vehicles move, need to be appropriately considered for the design of an effective VANET.

19. Explain in detail about Security issues.

Key Points

- Lack of physical boundary
- Low power RF transmissions
- Limited computational capabilities
- Limited power supply

Security Issues in a MANET

- MANETS are fundamentally different from both wired networks and infrastructure-based wireless networks.
- The nature of MANETs not only introduces new security concerns but also exacerbates the problem of detecting and preventing anomalous behaviour.
- In a wired network or in an infrastructure-based wireless network, an intruder is usually a host that is outside the network and therefore could be controlled through a firewall and subjected to access control and authentication.
- In a MANET, on the other hand, an intruder is part of the network, and therefore much more difficult to detect and isolate.
- Dynamic topological changes and the inherent wireless communications in a MANET, make it vulnerable to different types of attacks.
- Wireless links can get jammed and the batteries at the nodes can get depleted by such overloading, causing breakdowns of the network.
- Attackers can also disturb the normal operation of routing protocols by modifying the headers of packets.
- The intruder may insert spurious information while routing packets, causing erroneous routing table updates and thereby leading to frequent misroutings.

A few important characteristics of ad hoc networks that can be exploited to cause security vulnerabilities are the following:

Lack of physical boundary:
Each mobile node functions as a router and forwards packets from other nodes. As a result, network boundaries become blurred. The distinction between nodes that are internal or external to a network becomes meaningless, making it difficult to deploy firewalls or monitor the incoming traffic.

Low power RF transmissions:
It is possible for a malicious node to continuously transmit and monopolise the medium and cause its neighbouring nodes to wait endlessly for transmitting their messages. Also, signal jamming can lead to a denial-of-service (DoS) attack.

Limited computational capabilities:
Nodes in an ad hoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute-intensive security solutions such as setting up a public-key cryptosystem. Inability to encrypt messages invites a host of security attacks such as spoofing as well as several forms of routing attacks.

Limited power supply:
Since nodes normally rely on battery power, an attacker might attempt to exhaust batteries by causing unnecessary transmissions to take place or might cause excessive computations to be carried out by the nodes.

ANNA UNIVERSITY QUESTIONS

PART A

1. What is the key mechanism in mobile IP? [Nov 2018]
2. State the purpose of Home Location Register (HLR). [Nov 2018]
3. What is the purpose of DHCP? [Apr 2018]
4. What is the purpose of agent solicitation message? [Apr 2018]
5. To which layer do each of the following protocols belong to? What is their functionality? RARP, DNS [Nov 2017]
6. Differentiate the functionalities of a foreign agent and home agent.[Nov 2017]
7. What is Route Optimization? [May 2017]
8. List the modifications proposed in single-hop and multi-hop wireless network. [May 2017]
9. Define COA. [Nov 2016]
10. Illustrate the use of BOOTP protocol? [Nov 2016]
11. What is DHCP? [May 2016]
12. What is encapsulation in mobile IP? [May 2016]
13. Mention the two main design issues of MANET? [Nov 2018]
14. What are the important steps in destination sequence distance vector routing? [Nov 2018]
15. Compare VANET and MANET? [Apr 2018]
16. Differentiate cellular with adhoc networks? [Apr 2018]

17. List the applications of MANET's. [May 2017]
18. Distinguish proactive and reactive protocols. [May 2017]
19. Compare AODV and DSR protocols. [Nov 2017]
20. What are the contents of Link state Advertisement message? [Nov 2017]
21. Outline the concept of RTT? [Nov 2016]
22. Compare and contrast MANET Vs VANET [May 2016, Nov 2016]
23. List the characteristics of MANETs. [May 2016]

ANNA UNIVERSITY QUESTIONS

PART B

1. Explain about the key mechanism in Mobile IP. (16) [Nov 2016]
2. With a diagram explain DHCP and its protocol architecture. (8) [May 2016]
3. Explain IP in IP, minimal IP and GRE encapsulation methods. (8) [May 2016]
4. Illustrate packet delivery mechanism in mobile IP network with a neat Diagram. (16) [Nov 2017]
5. What is Encapsulation? Explain in detail the various encapsulation techniques in mobile IP. (16) [May 2017]
6. Explain mobile IP requirement and terminologies. (8) [Nov 2018]
7. Why the traditional IP cannot be used in the mobile network. In what way does mobile IP support mobile Hubs? (5) [Nov 2018]
8. Discuss Route Discovery and Route Maintenance mechanisms in DSR with Illustrations. List its merits and demerits. (16) [Nov 2017]
9. Describe the architecture of VANET with the functionality of the components. Compare VANET vs MANET. (16) [Nov 2017]
10. Explain the design issues of MANET routing protocols in detail. (16) [May 2017]
11. Explain any two VANET routing protocol with an example. (16) [May 2017]
12. Explain the Traditional Routing Protocols. (16) [Nov 2016]
13. What Multicast routing protocols. (8) [Nov 2016]
14. What are reactive and proactive protocols? Specify its advantages and Disadvantages. (8) [Nov 2016]

15. Explain characteristics, Applications of MANET. (4+4) [May 2016]
16. Explain DSR Routing Protocols in detail. (8) [May 2016]
17. Draw and explain the architecture of VANET. (8) [May 2016]
18. Explain the various security and attacks on VANET. (8) [May 2016]
19. Illustrate DSR routing in detail and compare it with DSDV. (13) [Nov 2018]
20. Explain the architecture of VANET and various security attacks on VANET. (13) [Nov 2018]
21. Describe the architecture of VANET with a neat diagram. (13) [Apr 2018]
22. Explain the design issues in MANET and the applications of adhoc network. (13) [Apr 2018]