educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

Unit 5

Mobile Network Layer

Mobile IP – Dynamic Host Configuration Protocol, Mobile Ad Hoc Routing Protocols– Multicast routing

Mobile IP – Dynamic Host Configuration Protocol, Mobile Ad Hoc:

- In response to the increasing popularity of palm-top and other mobile computers, Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one Internet attachment point to another.
- Although Mobile IP can work with wired connections, in which a computer is unplugged from one physical attachment point and plugged into another, it is particularly suited to wireless connections.
- The term mobile in this context implies that a user is connected to one or more applications across the Internet, that the user's point of attachment changes dynamically, and that all connections are automatically maintained despite the change.
- This is in contrast to a user, such as a business traveler, with a portable computer of some sort who arrives at a destination and uses the computer's notebook to dial into an ISP (Internet service provider). In this latter case, the user's Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back in.
- Each time an Internet connection is established, software in the point of attachment (typically an ISP) is used to obtain a new, temporarily assigned IP address. This temporary IP address is used by the user's correspondent for each application-level connection (e.g., FTP, Web connection). A better term for this kind of use is nomadic.

Operation of Mobile IP:

- Routers make use of the IP address in an IP datagram to perform routing. In particular, the network portion of an IP address (Figure 4.11) is used by routers to move a datagram from the source computer to the network to which the target computer is attached.
- Then the final router on the path, which is attached to the same network as the target computer, uses the host portion of the IP address to deliver the IP datagram to the destination. Further, this IP address is known to the next higher layer in the protocol architecture (Figure 4.1). In particular, most applications over the Internet are supported by TCP connections.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- When a TCP connection is set up, the TCP entity on each side of the connection knows the IP address of the correspondent host. When a TCP segment is handed down to the IP layer for delivery, TCP provides the IP address, and IP creates an IP datagram with that IP address in the IP header and sends the datagram out for routing and delivery.
- However, with a mobile host, the IP address may change while one or more TCP connections are active. Figure 12.1 shows in general terms how Mobile IP deals with the problem of dynamic IP addresses. A mobile node is assigned to a particular network, known as its home network. Its IP address on that network, known as its home address, is static.
- When the mobile node moves its attachment point to another network, that network is considered a foreign network for this host. Once the mobile node is reattached, it makes its presence known by registering with a network node, typically a router, on the foreign network known as a foreign agent.

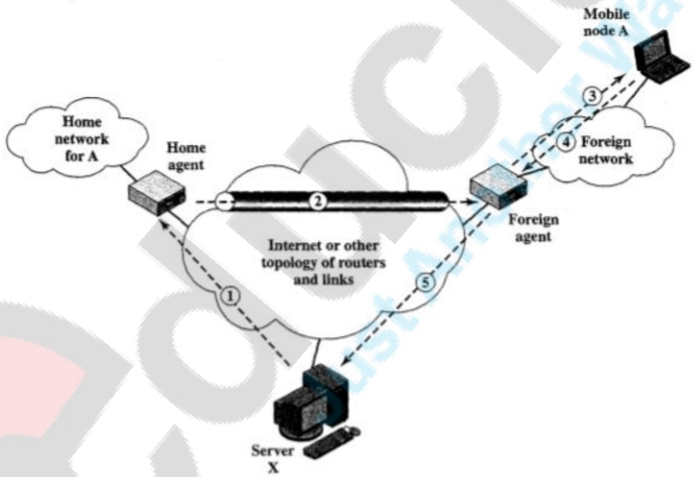


Figure 12.1 Mobile IP Scenario

- The mobile node then communicates with a similar agent on the user's home network, known as a home agent, giving the home agent the care-of address of the mobile node; the care-of address identifies the foreign agent's location.
- Typically, one or more routers on a network will implement the roles of both home and foreign agents.

When IP datagrams are exchanged over a connection between the mobile node and another host (a server in Figure 12.1), the following operations occur:

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

1. Server X transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.
2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram that has the A's care-of address in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as tunnelling. This IP datagram is routed to the foreign agent.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level PDU (e.g., a LAN LLC frame), and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it uses X's IP address. In our example, this is a fixed address; that is, X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network for routing to X. Typically, this router is also the foreign agent.
5. The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

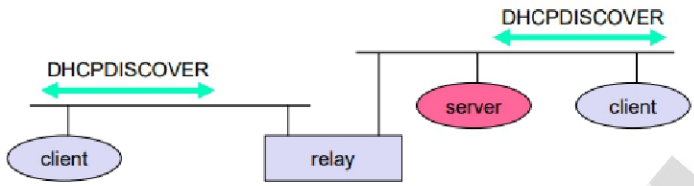
To support the operations illustrated in Figure 12.1, Mobile IP includes three basic capabilities:

- **Discovery:** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- **Registration:** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
- **Tunneling:** Tunneling is used to forward IP datagrams from a home address to a care-of address.

DHCP: Dynamic Host Configuration Protocol:

- Application:
  - If a new computer is connected to a network, DHCP provide it with all necessary information for full system integration into the network.
  - Supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  - Enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP
- Client/Server-Model:
  - The client sends via a MAC broadcast a request to the DHCP server: DHCP Discover.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more



DHCP Protocol:

DHCP uses a message exchange protocol over the UDP protocol

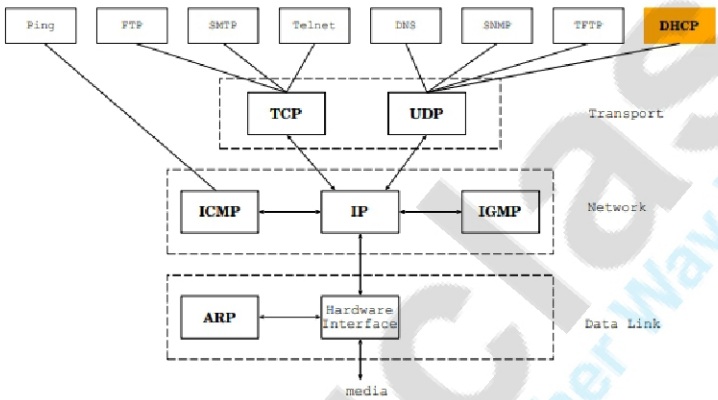


Figure 1.2: DHCP Protocol.

DHCP messages use the ports 67 and 68. Messages from a client to a server are sent to the 'server' port (67), while messages from a server to a client are sent to the 'client' port (68). The DCHP protocol essentially works as it.

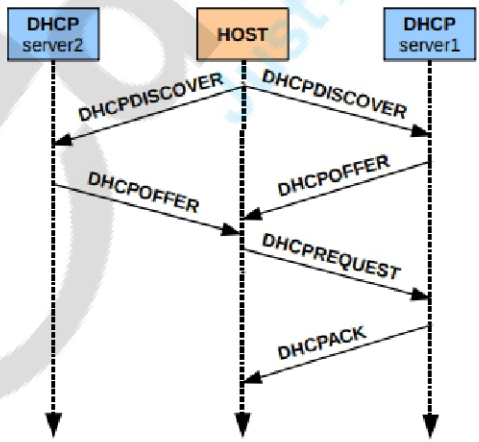


Figure 1.3: DHCP Protocol: Allocate an Address.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

To allocate a network address, the client broadcasts a DHCPDISCOVER message. Each DHCP server available in the network may respond with a DHCPOFFER message that includes an available network address and other configuration parameters. Then, the client selects a server and broadcasts a DHCPREQUEST message to request an IP address. The server sends a message (DHCPACK) with the requested parameters. The DHCP messages types are:

- ***DHCPDISCOVER*** Broadcasted by the client to locate available servers.
- ***DHCPOFFER*** Server to client in response to DHCPDISCOVER offering configuration parameters.
- ***DHCPREQUEST*** Client message to server's either
    a. Requesting offered parameters from one server and implicitly declining offers from all others,
    b. Confirming correctness of previously allocated address after, e.g., system reboot, or
    c. Extending the lease on a particular network address.
- ***DHCPACK*** Server to client with configuration parameters, including committed network address.
- ***DHCPNAK*** Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired
- ***DHCPDECLINE*** Client to server indicating network address is already in use.
- ***DHCPRELEASE*** Client to server relinquishing network address and cancelling remaining lease.
- ***DHCPINFORM*** Client to server, asking only for local configuration parameters; client already has externally configured network address. In Ethernet, the client uses the destination MAC to figure out which is the intended destination of the DHCP message. Finally, the messages between a client and a server use the same exchange identifier

DHCP characteristics:

- Server
    - Several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)
- Renewal of configurations
    - IP addresses have to be requested periodically, simplified protocol
- Options

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- Available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)
- Big security problems!
  - No authentication of DHCP information specified

educlash CGPA Convertor
Convert: SGPI->CGPA & PERCENTAGE / CGPA->PERCENTAGE
Visit educlash.com for more

Mobile Ad Hoc:

- An Ad hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support devices regularly available as conventional networks.
- These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighboring nodes in forwarding packets and hence the nodes in an Ad hoc network can act as both routers and hosts.
- Thus a node may forward packets between other nodes as well as run user applications. By nature these types of networks are suitable for situations where either no fixed infrastructure exists or deploying network is not possible.
- Ad hoc mobile networks have found many applications in various fields like military, emergency, conferencing and sensor networks. Each of these application areas has their specific requirements for routing protocols.
- Since the network nodes are mobile, an Ad hoc network will typically have a dynamic topology, which will have profound effects on network characteristics.
- Network nodes will often be battery powered, which limits the capacity of CPU, memory, and bandwidth. This will require network functions that are resource effective. Furthermore, the wireless (radio) media will also affect the behaviour of the network due to fluctuating link bandwidths resulting from relatively high error rates.
- These unique desirable features pose several new challenges in the design of wireless Ad hoc networking protocols. Network functions such as routing, address allocation, authentication and authorization must be designed to cope with a dynamic and volatile network topology.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- In order to establish routes between nodes, which are farther than a single hop, specially configured routing protocols are engaged.
- The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. In the simplest scenarios, nodes may be able to communicate directly with each other, for example, when they are within wireless transmission range of each other.
- However, Ad hoc networks must also support communication between nodes that are only indirectly connected by a series of wireless hops through other nodes.
- For example, in Fig 3.1, to establish communication between nodes A and C the network must enlist the aid of node B to relay packets between them.
- The circles indicate the nominal range of each node's radio transceiver. Nodes A and C are not in direct transmission range of each other, since A's circle does not cover C.

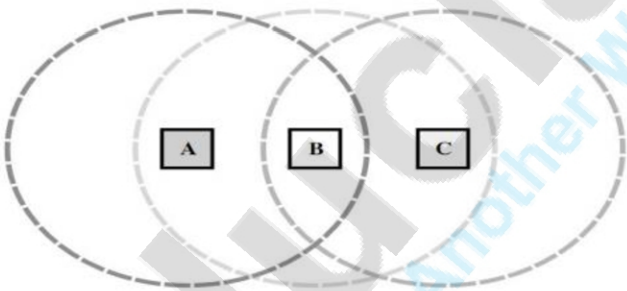


Figure 3.1: A Mobil Ad hoc network of three nodes, where nodes A and C must discover the route through B in order to communicate.

- In general, an Ad hoc network is a network in which every node is potentially a router and every node is potentially mobile. The presence of wireless communication and mobility make an Ad hoc network unlike a traditional wired network and requires that the routing protocols used in an Ad hoc network be based on new and different principles.
- Routing protocols for traditional wired networks are designed to support tremendous numbers of nodes, but they assume that the relative position of the nodes will generally remain unchanged.

FEATURES OF MOBILE AD HOC NETWORKS:

The mobile Ad hoc networks has the following features-

- Autonomous terminal
- Distributed operation

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- Multihop routing
- Dynamic network topology
- Fluctuating link capacity
- Light-weight terminals

1. **Autonomous Terminal:**
   In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, beside the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
2. ***Distributed Operation:***
   Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed to implement functions like security and routing.
3. ***Multihop Routing:***
   Basic types of Ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the lesser cost of functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
4. ***Dynamic Network Topology:***
   Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the Ad hoc network, but may require access to a public fixed network (e.g. Internet)
5. ***Fluctuating Link Capacity:***
   The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

The channel over which the terminals communicate is subjected to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

6. ***Light Weight Terminals:***
   In most of the cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

CHALLENGES OF MOBILE AD HOC NETWORKS:

Ad hoc networking has been a popular field of study during the last few years. Almost every aspect of the network has been explored in one way or other at different level of problem. Yet, no ultimate resolution to any of the problems is found or, at least, agreed upon. On the contrary, more questions have arisen. The topics that need to be resolved are as follows:

- Scalability
- Routing
- Quality of service
- Client server model shift
- Security
- Energy conservation
- Node cooperation
- Interoperation

1. ***Scalability:***
   Most of the visionaries depicting applications which are anticipated to benefit from the Ad hoc technology take scalability as granted. Imagine, for example, the vision of ubiquitous computing where networks can be of "any size". However, it is unclear how such large networks can actually grow.
   Ad hoc networks suffer, by nature, from the scalability problems in capacity. To exemplify this, we may look into simple interference studies. In a non-cooperative network, where omni-directional antennas are being used, the throughput per node decreases at a rate $1/\sqrt{N}$, where N is the number of nodes. That is, in a network with 100 nodes, a single device gets, at most, approximately one tenth of the theoretical network data rate.
   This problem, however, cannot be fixed except by physical layer improvements, such as directional antennas. If the available capacity

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

like bandwidth, radiation pattern of antenna sets some limits for communications. This demands the formulation of new protocols to overcome circumvents. Route acquisition, service location and encryption key exchanges are just few examples of tasks that will require considerable overhead as the network size grows.
If the scarce resources are wasted with profuse control traffic, these networks may see never the day dawn. Therefore, scalability is a boiling research topic and has to be taken into account in the design of solutions for Ad hoc networks.

2. ***Routing:***
Routing in wireless Ad hoc networks is nontrivial due to highly dynamic environment. An Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any pre-existing network infrastructure or centralized administration.
In a typical Ad hoc network, mobile nodes come together for a period of time to exchange information. While exchanging information, the nodes may continue to move, and so the network must be prepared to adapt continually to establish routes among themselves without any outside support.
3. ***Quality of Service:***
The heterogeneity of existing Internet applications has challenged network designers who have built the network to provide best-effort service only. Voice, live video and file transfer are just a few applications having very diverse requirements.
Qualities of Service (QoS) aware solutions are being developed to meet the emerging requirements of these applications.
QoS has to be guaranteed by the network to provide certain performance for a given flow, or a collection of flows, in terms of QoS parameters such as delay, jitter, bandwidth, packet loss probability, and so on. Despite the current research efforts in the QoS area, QoS in Ad hoc networks is still an unexplored area.
Issues of QoS in robustness, QoS in routing policies, algorithms and protocols with multipath, including preemptive, priorities remain to be addressed.
4. ***Client-Server Model Shift:***
In the Internet, a network client is typically configured to use a server as its partner for network transactions. These servers can be found automatically or by static configuration.
In Ad hoc networks, however, the network structure cannot be defined by collecting IP addresses into subnets. There may not be servers, but the demand for basic services still exists.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

Address allocation, name resolution, authentication and the service location itself are just examples of the very basic services which are needed but their location in the network is unknown and possibly even changing over time. Due to the infrastructure less nature of these networks and node mobility, a different addressing approach may be required. In addition, it is still not clear who will be responsible for managing various network services.

Therefore, while there have been vast research initiatives in this area, the issue of shift from the traditional client-server model remains to be appropriately addressed.

5. ***Security:***

   A vital issue that has to be addressed is the Security in Ad hoc networks. Applications like Military and Confidential Meetings require high degree of security against enemies and active/passive eavesdropping attacker.

   Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures very vulnerable to infiltration, eavesdropping, interference, and so on.

   Security is often considered to be the major "roadblock" in the commercial application.

6. ***Energy Conservation:***

   Energy conservative networks are becoming extremely popular within the Ad hoc networking research. Energy conservation is currently being addressed in every layer of the protocol stack.

   There are two primary research topics which are almost identical: maximization of lifetime of a single battery and maximization of the lifetime of the whole network. The former is related to commercial applications and node cooperation issues whereas the latter is more fundamental, for instance, in military environments where node cooperation is assumed.

   The goals can be achieved either by developing better batteries, or by making the network terminals operation more energy efficient. The first approach is likely to give a 40% increase in battery life in the near future (with Li-Polymer batteries).

   As to the device power consumption, the primary aspect are achieving energy savings through the low power hardware development using techniques such as variable clock speed CPUs, flash memory, and disk spin down

7. ***Node (MH) Cooperation:***

   Closely related to the security issues, the node cooperation stands in the way of commercial application of the technology. To receive the

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

corresponding services from others there is no alternative but one has to rely on other people's data.

However, when differences in amount and priority of the data come into picture, the situation becomes far more complex. A critical fire alarm box should not waste its batteries for relaying gaming data, nor should it be denied access to other nodes because of such restrictive behavior.

Encouraging nodes to cooperate may lead to the introduction of billing, similar to the idea suggested for Internet congestion control. Well-behaving network members could be rewarded, while selfish or malicious users could be charged higher rates.

Implementation of any kind of billing mechanism is, however, very challenging. These issues are still wide open

8. ***Interoperation:***

The self-organization of Ad hoc networks is a challenge when two independently formed networks come physically close to each other. This is an unexplored research topic that has implications on all levels on the system design.

When two autonomous Ad hoc networks move into same area the interference with each other becomes unavoidable. Ideally, the networks would recognize the situation and be merged. However, the issue of joining two networks is not trivial; the networks may be using different synchronization, or even different MAC or routing protocols. Security also becomes a major concern.

Can the networks adapt to the situation? For example; a military unit moving into an area covered by a sensor network could be such a situation; moving unit would probably be using different routing protocol with location information support, while the sensor network would have a simple static routing protocol.

Another important issue comes into picture when we talk about all wireless networks. One of the most important aims of recent research on all wireless networks is to provide seamless integration of all types of networks. This issue raises questions on how the Ad hoc network could be designed so that they are compatible with wireless LANs, 3 Generation (3G) and 4G cellular networks.

Routing Protocols– Multicast routing:

Multicast Routing Protocols:

Multicasting is the process of sending packets from a transmitter to multiple destinations identified by a single address. As with their wired counterparts, multicasting in MANET is also a hard task to accomplish, and it is even harder in the MANET case since the physical topology changes quite

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

frequently. Therefore, multicast protocols designed for a MANET have to take topological changes into consideration. In this section, we discuss two multicast routing protocols, namely AODV Multicasting and ODMRP, proposed within the MANET [MANET] working group at the IETF [IETF].

1. **Destination sequence distance vector**
   - **Destination sequence distance vector (DSDV)** routing is an enhancement to distance vector routing for adhoc networks.
   - DSDV can be considered historically.
   - Distance vector routing is used as routing information protocol (RIP) in wired networks.
   - It performs extremely poorly with certain network changes dueto the count-to-infinity problem.
   - Each node exchanges its Neighbor table periodically with its neighbors.
   - Changes at one node in the network propagate slowly through the network.

DSDV now adds two things to the distance vector algorithm:

- **Sequence numbers:**
  - Each routing advertisement comes with a sequence number.
  - Within ad-hoc networks, advertisements may propagate along many paths.
  - Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.
- **Damping:**
  - Transient changes in topology that are of short duration should not destabilize the routing mechanisms.
  - Advertisements containing changes in the topology currently stored are therefore not disseminated further.
  - A node waits with dissemination if these changes are probably unstable.
  - Waiting time depends on the time between the first and the best announcement of a path to a certain destination.

2. **Dynamic source routing**

- Imagine what happens in an ad-hoc network where nodes exchange packets from time to time, i.e., the network is only lightly loaded, and DSDV or one of the traditional distance vector or link state algorithms is used for updating routing tables.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- Although only some user data has to be transmitted, the nodes exchange routing information to keep track of the topology. These algorithms maintain routes between all nodes, although there may currently be no data exchange at all. This causes unnecessary traffic and prevents nodes from saving battery power.

Table 8.2 Part of a routing table for DSDV

Destination	Next hop	Metric	Sequence no.	Instal time
N_1	N_1	0	S_1–321	T_4–001
N_2	N_2	1	S_2–218	T_4–001
N_3	N_2	2	S_3–043	T_4–002
N_4	N_4	1	S_4–092	T_4–001
N_5	N_4	2	S_5–163	T_4–002

Applying route discovery to the example in Figure 8.20 for a route from N1 to N3 at time t1 results in the following.

- N1 broadcasts the request ((N1), id = 42, target = N3), N2 and N4 receive this request.
- N2 then broadcasts ((N1, N2), id = 42, target = N3), N4 broadcasts ((N1, N4), id = 42, target = N3). N3 and N5 receive N2's broadcast, N1, N2, and N5 receive N4's broadcast.
- N3 recognizes itself as target, N5 broadcasts ((N1, N2, N5), id = 42, target =N3). N3 and N4 receive N5's broadcast.
- N1, N2, and N5 drop N4's broadcast packet, because they all recognize an already received route request (and N2's broadcast reached N5 before N4's did). N4 drops N5's broadcast, N3 recognizes (N1, N2, N5) as an alternate, but longer route.
- N3 now has to return the path (N1, N2, N3) to N1. This is simple assuming symmetric links working in both directions. N3 can forward the information using the list in reverse order.

- **Dynamic source routing (DSR)**, therefore, divides the task of routing into two separate problems (Johnson, 1996), (Johnson, 2002):
  - **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
  - **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.
- The basic principle of source routing is also used in fixed networks, e.g. token rings.
- Dynamic source routing eliminates all periodic routing updates and works as follows.

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters.
- Anynode that receives a route request does the following.
  - If the node has already received the request (which is identified using the unique identifier), it drops the request packet.
  - If the node recognizes its own address as the destination, the request has reached its target.
  - Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.
- Using this approach, the route request collects a list of addresses representing a possible path on its way towards the destination.
- As soon as the request reaches the destination, it can return the request packet containing the list to the receiver using this list in reverse order.

3. Alternative metrics:

- One other metric, called **least interference routing** (LIR), takes possible interference into account.
- Figure 8.21 shows an ad-hoc network topology.
- SenderS1 wants to send a packet to receiver R1, S2 to R2.
- Using the hop count as metric,S1 could choose three different paths with three hops, which is also the minimum.
- Possible paths are (S1, N3, N4, R1), (S1, N3, N2, R1), and (S1, N1, N2, R1).
- S2 would choose the only available path with only three hops (S2, N5, N6, R2).
- Taking interference into account, this picture changes.

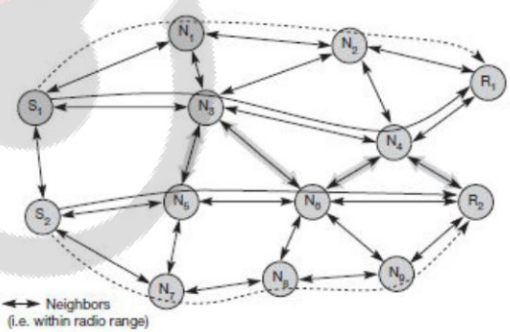


Figure 8.21
Example for least interference routing

educlash Result / Revaluation Tracker
Track the latest Mumbai University Results / Revaluation as they happen, all in one App
Visit educlash.com for more

- To calculate the possible interference of a path, each node calculates its possible interference (interference is defined here as the number of neighbours that can overhear a transmission).
- Every node only needs local information to compute its interference.
- In this example, the interference of node N3 is 6, that of node N4 is 5 etc.
- Calculating the costs of possible paths between S1 and R1 results in the following:
  C1 = cost(S1, N3, N4, R1) = 16,
  C2 = cost(S1, N3, N2, R1) = 15,
  and C3 = cost(S1, N1, N2, R1) = 12.
- All three paths have the same number of hops, but the last path has the lowest cost due to interference.
- Thus, S1 chooses (S1, N1, N2, R1). S2 also computes the cost of different paths, examples are C4 = cost(S2, N5, N6, R2) = 16 andC5 = cost(S2, N7, N8, N9, R2) = 15. S2 would, therefore, choose the path (S2, N7,N8, N9, R2), although this path has one hop more than the first one.
- With both transmissions taking place simultaneously, there would have been interference between them as shown in Figure 8.21.
- In this case, least interference routing helped to avoid interference.
- Taking only local decisions and not knowing what paths other transmissions take, this scheme can just lower the probability of interference.
- Interference can only be avoided if all senders know of all other transmissions (and the whole routing topology) and base routing on this knowledge.
- Routing can take several metrics into account at the same time and weigh them.
- Metrics could be the number of hops h, interference i, reliability r, errorrate e etc. The cost of a path could then be determined as:
  $$\text{cost} = \alpha h + \beta i + \gamma r + \delta e + \ldots$$
- It is not at all easy (if even possible) to choose the weights $\alpha, \beta, \gamma, \delta, \ldots$ to achieve the desired routing behavior.

educlash CGPA Convertor
Convert: SGPI->CGPA & PERCENTAGE / CGPA->PERCENTAGE
Visit educlash.com for more