UNIT IV

Adhoc Basic Concepts

Ad hoc networks, which are also called mesh networks, are defined by the manner in which the network nodes are organized to provide pathways for data to be routed from the user to and from the desired destination. Actually, the two names ascribed to these networks provide considerable insight. Ad hoc has two definitions—the first can be either "impromptu" or "using what is on hand," while the other is "for one specific purpose." For example, members of an ad hoc committee (studying a specific issue) might discover that they are attending the same event and decide to have an ad hoc (impromptu) meeting

Advantages of Ad Hoc Networks The principal advantages of an ad hoc network include the following: • Independence from central network administration • Self-configuring, nodes are also routers • Self-healing through continuous re-configuration • Scalable—accommodates the addition of more nodes • Flexible—similar to being able to access the Internet from many different locations

Limitations of Ad Hoc Networks While ad hoc networks are typically used where they have the greatest emphasis on its advantages, there are some limitations: • Each node must have full performance • Throughput is affected by system loading • Reliability requires a sufficient number of available nodes. Sparse networks can have problems • Large networks can have excessive latency (time delay), which affects some applications.

MANET: 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

FEATURES OF MOBILE AD HOC NETWORKS The mobile Ad hoc networks has the following features- Autonomous terminal• Distributed operation• Multihop routing• Dynamic network topology• Fluctuating link capacity• Light-weight terminals•

Characteristics to design on a MANET:

Lack of fixed infrastructure: A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be uni directional (broadcast), highly- directional (point-to-point). At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.--is often much less than a radio's maximum transmission rate.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation due to substantial amount of energy causing the batteries to get rapidly drained out unless the protocol is carefully designed.

Increased vulnerability: Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

MANET Applications:

APPLICATIONS OF AD HOC NETWORKS Ad hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective .The following are some of the important applications. Business Applications

One of many possible uses of mobile Ad hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment. Work has been going on to introduce the fundamental concepts of game theory and its applications in telecommunications. Game theory originates from economics and has been applied in various fields. Game theory deals with multi-person decision making, in which each decision maker tries to maximize his utility. The cooperation of the users is necessary to the operation of Ad hoc networks; therefore, game theory provides a good basis to analyze the networks. People playing multi-player games usually do so over the Internet, with a remote host. This model is called the client-server model. In the case of multiple users, each user just connects to a common server, and the server forwards the packets to connected users. Fig 3.2 illustrates the client-server model.

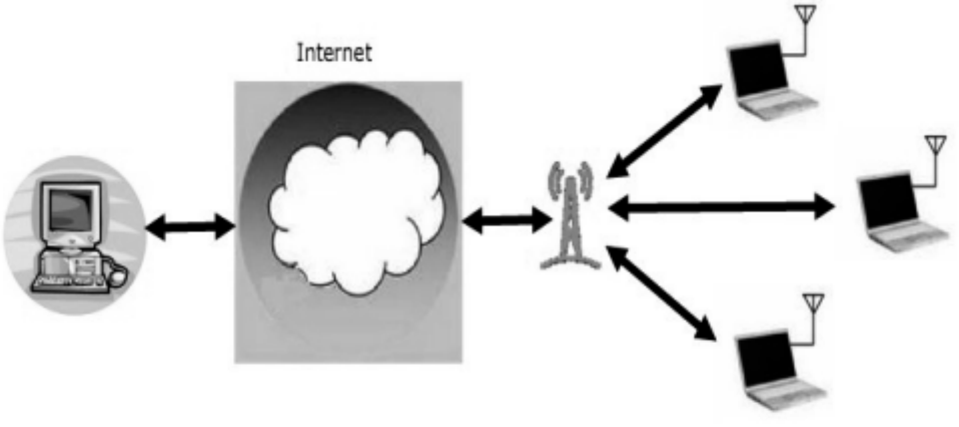


Fig 3.2: Client-Server Model

Military Applications :Military applications have motivated early research on Ad hoc networks. The ability to quickly set up a network among military units in hostile territory without any infrastructure support can provide friendly forces with a considerable tactical advantage on the battlefield. For instance, each soldier can carry a mobile device that represents one of the mobile nodes in an Ad hoc network linking all soldiers, tanks, and other vehicles as shown in Fig 3.3. Recent advances in robotics have also motivated the idea of automated battlefields in which unmanned fighting vehicles are sent into battle. Supporting military applications requires self-organizing mechanisms that provide robust and reliable communication in dynamic battle situations.

Fig 3.3: Soldiers, Tanks and other Vehicles carrying Mobile Devices

Emergency Operations Another promising application area for Ad hoc networks is emergency services, including search and rescue and disaster recovery operations. As an example of search and rescue, consider an airline that attaches small wireless devices to the life jackets under each seat. Suppose that the plane has mechanical problems and has to make an emergency landing in the water. Once search and rescue teams arrive at the landing site, they are provided with detailed information about the location (the coordinates and potentially the depth) of the victims through the transponders. As a result, the rescue teams can more effectively locate and reach the victims. The mobile devices could also monitor the vital signs of victims, such as heart rate or breathing rate, to prioritize the rescue of victims that are still alive

Home, Office, and Educational Applications Ad hoc networks also have applications in home and office environments. The simplest and most direct application of Ad hoc networks in both homes and offices is the networking of laptops, PDAs and other WLAN-enabled devices in the absence of a wireless base station. Another home application that falls within the Personal Area Network (PAN) class is wire replacement through wireless links, as in Bluetooth. All periphery devices can connect to a computer through wireless Bluetooth links, eliminating the need for wired connections. Ad hoc networks can also enable streaming of video and audio among wireless nodes in the absence of any base station. For instance, UWB provides a sufficiently high bandwidth (in the order of Gb/s) to support several multimedia streams. UWB-equipped nodes can autonomously set up an Ad hoc network to stream high quality video and audio between several computers through wireless UWB connections. Educational and recreational activities can also benefit from Ad hoc networks. For example, students attending a classroom can use their laptops to obtain the latest class material from a professor's laptop as the class progresses. Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures are some of the educational applications of Ad hoc networks. On the recreational side, the mobility and nomadic nature of Ad hoc networks enables richer multi-user games that can incorporate user mobility and proximity into the virtual game environment.

MANET design issue:

Network Size and Node Density: 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. The cluster size Depend on node density.

Connectivity: The Term connectivity of a node usually refers to the number of neighbors it has. Connectivity between two nodes also sometimes used to refer to a link between the two nodes. The term link capacity denotes the bandwidth of the link.

Network Topology: The topology of a network denoted connectivity among the various nodes of thee network. The mobility of the nosed affects a network topology. Other than mobility nodes can become in operative due to discharge batteries or hardware failures, and thereby causing changes topology. It should be appropriate in design of Network.

User Traffic: The traffic in a network can be various types: They are Bur sty Traffic, Large packet sent periodically, Combinations of the above two Types.

Operational Environment: The operational environment supports the Line of Sight (LOS) Communication. But there can be significant difference in the node density and mobility values in different operational environments requiring different design of mobile network to suit an operational environment.

Energy constraint: There is no fixed infrastructure exist in a MANET. The Mobile node 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 indispensible if the network is to be kept operational the energy spent can be substantially reduced by allowing the nodes to go into a sleep node whenever possible.

Routing

The purpose of routing is to find the best path between the source and destination for forwarding packets in any store and forward network. It is necessary to find a new route each time a node needs to transmit a message making routing an expensive and difficult task. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path

Forward the packet to the next hop

While forwarding, the sender needs to ensure that

- The packet moves towards its destination
- The number of hop/path length is minimized.
- Delay is minimized
- The packet loss is minimized
- The packet does not move around the network endlessly

The term link denotes the connection of one router to its neighboring router. A neighbor of a router is one with which it can directly communicate without taking any help from any of the intervening routers. Each router determines its local connectivity information and flood the network with this information with Link state advertisement. As a router in the network receives this Link state advertisement it stores this packet in a link state packet Data Base (LSPDB).. The storage of link state advertisement in an LSPDB is in addition to the routing table that each router maintains. All routers in the network have identical LSPBDs.. Based on the bits and piece of information stored in the LSPDB, each router construct the connectivity information for the entire network as a graph using Dijastras Shortest Path Algorithm.. Once a router construct this graph it computes the routing table from this and uses in all its routing decision. Thus Routing in the LSP bases its routing decision on message s received from other routers in the network regarding their link state or the state of this connectivity with other routers. The basic characteristics of LSP is that every router construct a graph representing the connectivity between the various nodes in the network based on the information received from other routers.

Link State routing protocol

In a Link state protocol each router periodically determines the state of its neighbors by exchanging hello packets with them across all its network interfaces.. A router is connected to the other routers through link established by its network interface. Based on the reply received from its neighbors the router determines the state of the link in terms of the delay and other characteristics. Subsequently the router forms a short message called the link state advertisement and sends to its neighbors.. A link state advertisement is also sent by router whenever it experiences any connectivity changes. The Link state advertisement messages are usually the following:

The identity of the router originating the message

The identities of all its neighbors

The delay along various links to its neighbors

A unique sequence number formed by increasing the count every time the router forms a new link state advertisement.

The LS advertisement is then flooded throughout the Network as follows

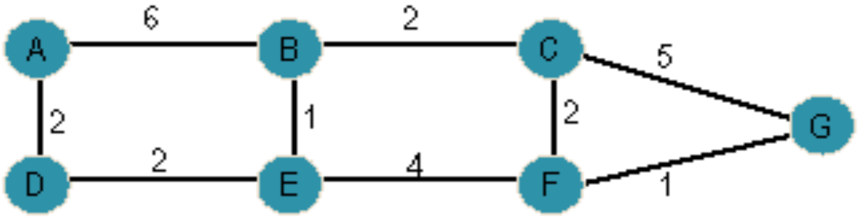
A router sends a copy of a link state advertisement to all of its neighbors. A router receiving this message examines the sequence number of the last link state advertisement from the originating router by consulting its LSPDB. It is recent it replaces the last message with the currently received message in its LSPDB and also forwards a copy of this link state advertisement to each of its neighbors.

Construction of Link state Tree: A router maintains two data structure tree containing nodes which are done and a list of candidates..This tree is essentially a shortest path first (SPF) tree.

- All routers which are connected to the router just added to the tree, excepting any Routers which are either already present in the tree or in the candidate list, are added To the candidate list.
- The delay from each router in the candidate list to every other router in the tree are compared.
- Greedy iterative Algorithm: All routes are connected to the router just added to the tree excepting any routers which are either already present in the tree or in the candidate list are added to the candidate list.
- The delay from each router in the candidate list to every other router in the tree is compared. The candidate router having the shortest delay is moved into the tree and attached to the appropriate neighbor router. Whenever a router is moved from the candidate list into the tree it is removed from the candidate list.

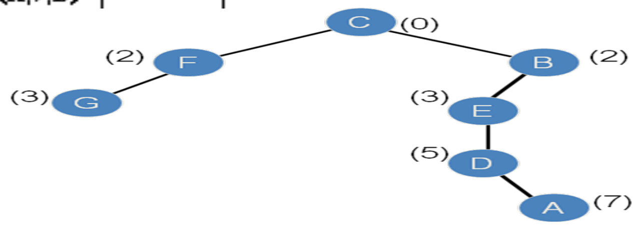
The above two steps are repeated till there are no more routers left in the candidate list.. If different routers somehow have maps that are inconsistent the routing loops can form.

Example:



STEP	Confirmed	Tentative	Comments
1	(C, 0,-)		Only C is added in the confirmed list. Look through C's LSP
2	(C, 0,-)	(F,2,_) (G,5,_) (B,2,_)	C's LSP says F can be reached with cost 2 & G can be reached with cost 5 & B can be reached with cost 2 All these routes are put in Tentative as no better option is known
3	(C, 0,-) (F,2,_)	(G,5,_) (B,2,_)	The node F with the lowest cost is added to Confirmed list. Look through F's LSP
4	(C, 0,-) (F,2,_)	(G,5,_) (B,2,_) (G,3,F) (E,6,F)	F's LSP says G can be reached with cost 3 from C through F& E can be reached with cost 6 from C through F All these routes are put in Tentative
5	(C, 0,-) (F,2,_) (B,2,_)	(G,5,_) (G,3,F) (E,6,F)	Move (B,2,_) from tentative list to confirmed list Look through the LSP of B
6	(C, 0,-) (F,2,_) (B,2,_)	(G,5,_) (G,3,F) (E,6,F) (E,3,B) (A,6,B)	B's LSP says E can be reached with cost 3 from C through B& A can be reached with cost 8 from C through B
6	(C, 0,-) (F,2,_) (B,2,_) (G,3,F)	(E,6,F) (E,3,B) (A,8, B)	(G,5,_) is compared with new (G,3,F) The lowest cost path (G,3,F)is added to Confirmed list (G,5,_) is removed from the Tentative list Look through G's LSP
7	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B)	(A,8,B)	All G's LSP (F and C) are already in Confirmed list (E,6,F) is compared with new (E,3,B) The lowest cost path (E,3,B))is added to Confirmed list (E,6,F) is removed from the Tentative list Look through E's LSP
8	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B)	(A,8,B) (D,5,E)	E's LSP says D can be reached with cost 5 from C through E
9	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B) (D,5,E)	(A,8,B) (A,7,D)	Add (D,5,E) as there is no better option Look through E's LSP. It says D 's LSP says A can be reached with cost 7 through D. Add (A,7,D) to the Tentative list
10	(C, 0,-) (F,2,_) (B,2,_) (G,3,F) (E,3,B) (D,5,E) (A,7,D)		The least cost route (A,7,D) is moved to the confirmed list

- We can now create a forwarding database:



Forwarding Database		
Dest	Next HOP	Cost
C	C	0
F	F	2
G	F	3
B	B	2
E	B	3
D	B	5
A	B	7

Distance Vector protocol

Distance Vector Routing :Each node constructs a one-dimensional array (a vector) containing the “distances” (costs) to all other nodes.

distributes that vector to its immediate neighbors.

- Each node knows the cost of the link to each of its directly connected neighbors.
- A link that is down/unknown is assigned an infinite cost.

PRINCIPLE: Constructing RIP message

Step 1: Each node sets a cost of 1 (one) to all directly connected neighbors and cost of ∞ to others in the neighbors.

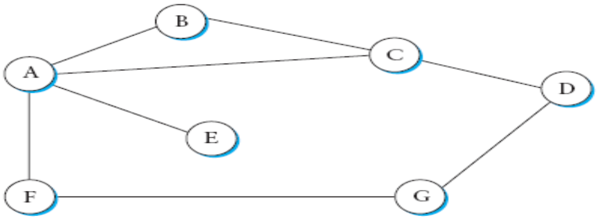
Step 2: Each node sends a message to its directly connected neighbor s containing its knowledge of distances of all nodes in the network.

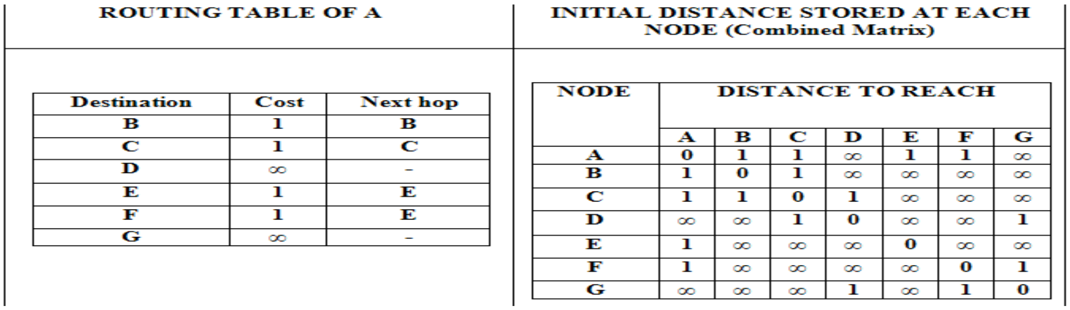
Repeat the following steps for each advertised destination:

1. If (destination not in the routing table)

```
        Add the advertised information to the table by adding
       the two costs
     2. Else (
   one. (Because this may be new)
          Else (next-hop field destination in the routing table)
          If (next-hop field is the same) Replace entry in the
      table with the advertised is not the same)
          If (advertised hop count smaller than one in
         the table) Replace entry in the routing table. (better one
3. Return.
```

- Initially, each node sets a cost of 1 to its directly connected neighbors and ∞ to all other nodes.
- Thus, A initially believes that it can reach B ,C, E, F in one hop and that D is unreachable.





ROUTING TABLE OF A

Destination	Cost	Next hop
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	E
G	∞	-

INITIAL DISTANCE STORED AT EACH NODE (Combined Matrix)

NODE	DISTANCE TO REACH						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Proactive routing protocol

Proactive protocols: In networks utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain a up-to-date routing information from each node to every other node.

Reactive(On Demand)

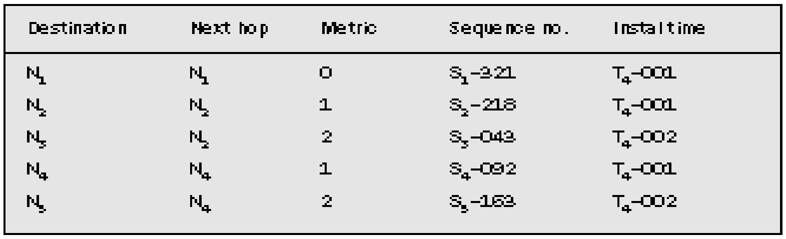
- Do not maintain the network topology information & the nodes do not exchange routing information periodically.
- They obtain the necessary path when required by using a con establishment process.
- Executes the path finding process & exchange routing information only when a path is required by a node to communicate with a destination.

DESTINATION SEQUENCE DISTANCE VECTOR (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks (Perkins, 1994). DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols currently discussed (see section 8.3.5). Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to 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 (step-by-step with every exchange). The strategies to avoid this problem which are used in fixed networks (poisoned-reverse/split horizon (Perlman, 1992)) do not help in the case of wireless ad-hoc networks, due to the rapidly changing topology. This might create loops or unreachable regions within 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.



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

For each node N1 stores

- the toward this node,
- the metric (next hop here number of hops),
- the sequence number of the last advertisement for this node,
- the time at which the path has been installed first.

The table contains flags and a settling time helping to decide when the path can be assumed stable. Router advertisements from N1 now contain data from the first, third, and fourth column: destination address, metric, and sequence number. Besides being loop-free at all times, DSDV has low memory requirements and a quick convergence via triggered updates.

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. 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.

- **Dynamic source routing (DSR)**, therefore, divides the task of routing into two separate problems:
- **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.

If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any node 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. One condition for this is that the links work bi-directionally. If this is not the case, and the destination node does not currently maintain a route back to the initiator of the request, it has to start a route discovery by itself. The destination may receive several lists containing different paths from the initiator. It could return the best path, the first path, or several paths to offer the initiator a choice. 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.

The assumption of bi-directional links holds for many ad-hoc networks. However, if links are not bi-directional, the scenario gets more complicated. The algorithm has to be applied again, in the reverse direction if the target does not maintain a current path to the source of the route request.

● N3 has to broadcast a route request ((N3), id = 17, target = N1). Only N5 receives this request.

● N5 now broadcasts ((N3, N5), id = 17, target = N1), N3 and N4 receive the broadcast.

● N3 drops the request because it recognizes an already known id. N4 broadcasts ((N3, N5, N4), id = 17, target = N1), N5, N2, and N1 receive the broadcast.

● N5 drops the request packet, N1 recognizes itself as target, and N2 broadcasts ((N3, N5, N4, N2), id = 17, target = N1). N3 and N5 receive N2's broadcast.

● N3 and N5 drop the request packet.

Now N3 holds the list for a path from N1 to N3, (N1, N2, N3), and N1 knows the path from N3 to N1, (N3, N5, N4, N1). But N1 still does not know how to send data to N3! The only solution is to send the list (N1, N2, N3) with the broadcasts initiated by N3 in the reverse direction. This example shows clearly how much simpler routing can be if links are symmetrical. The basic algorithm for route discovery can be optimized in many ways.

● To avoid too many broadcasts, each route request could contain a counter. Every node rebroadcasting the request increments the counter by one. Knowing the maximum network diameter (take the number of nodes if nothing else is known), nodes can drop a request if the counter reaches this number.

● A node can cache path fragments from recent requests. These fragments can now be used to answer other route requests much faster (if they still reflect the topology!).

● A node can also update this cache from packet headers while forwarding other packets.

● If a node overhears transmissions from other nodes, it can also use this information for shortening routes.

After a route has been discovered, it has to be maintained for as long as the node sends packets along this route. Depending on layer two mechanisms, different approaches can be taken. If the link layer uses an acknowledgement the node can interpret this acknowledgement as an intact route.

● If possible, the node could also listen to the next node forwarding the packet, so getting a passive acknowledgement.

● A node could request an explicit acknowledgement. Again, this situation is complicated if links are not bi-directional. If a node detects connectivity problems,

- It has to inform the sender of a packet, initiating a new route discovery starting from the sender.

- Alternatively, the node could try to discover a new route by itself.

Although dynamic source routing offers benefits compared to other algorithms by being much more bandwidth efficient, problems arise if the topology is highly dynamic and links are asymmetrical.

i) AODV

- Ad Hoc On-demand Distance Vector
- Source floods route request in the network.
- Reverse paths are formed when a node hears a route request.
- 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.
- Each node forwards the request only once (pure flooding).
- Each route has a lifetime after which the route expires if it is not used.
- A route is used.

only when it is used and hence old and expired routes are never ns only one route between a source-destination pair.

(ii) Zone routing

Zone Routing is a hybrid protocol. It incorporates the merits of both on demand and proactive routing protocols.

- Routing zone comprise a few MANET notes within a few hops from the central zone.

Zone Routing is a hybrid protocol. It incorporate the merits of both on demand and proactive routing protocol. A routing zone is similar to a cluster. A routing zone comprises a few MANET nodes within a few hops from the central zone. Within a central zone, table-driven routing protocol is used. Each node therefore has a route to all other nodes within the zone. If a destination node happens to be outside the sources zone's employs an on demand route discovery procedure which works.

- If a packet's destination is in the same zone as the origin, the proactive protocol using an already stored routing table is used to deliver the packet immediately.
- If the route extends outside the packet's originating zone, a reactive protocol takes over to check each successive zone in the route to see whether the destination is inside that zone.
- This reduces the processing overhead for those routes. Once a zone is confirmed as containing the destination node, the proactive protocol, or stored route-listing table, is used to deliver the packet.

Multicast routing

- Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters
- Efficient delivery to multiple destinations
- (e.g. video broadcast)
- IP Multicast service model
- Communications based on groups
- Special IP addresses (Class D in IPv4) represent "multicast groups"

- Anyone can join group to receive packets Anyone can send to group Sender need not be part of group
- Dynamic group membership – can join and leave at will Unreliable datagram service
- Extension to unicast IP
- Group membership not visible to hosts
- No synchronization

VANET

In VANETs, wireless communication has been a critical technology to support the achievement of many applications and services. However, due to the characteristics of VANETs such as high dynamic topology and intermittent connectivity, the existing routing algorithms in MANETs are not available for most application scenarios in VANETs.

- Driver and Vehicle Model. This model aims to reflect the behaviour of a single vehicle. This behavior needs to consider two main factors: different driving styles and the vehicle characteristics, such as an aggressive or passive driver and a sports car.
- Traffic Flow Model. This model aims to reflect interactions between vehicles, drivers, and infrastructures and develop an optimal road network. In [31], according to various criteria (level of detail, etc.), the authors discuss three classes of traffic flow models: microscopic, microscopic, and macroscopic.
- Communication Model. This model is a pretty important part of research methodologies to address the data exchange among the road users. Thanks to the constraints of many factors (the performance of the different communication layers, communication environment, and the routing strategies), communication model plays an important role in the research. The authors in [17] give a detailed overview in the research field.(iv)Application Model. This model is very useful for the market introduction because it can address the behaviour and quality of cooperative VANETs applications.

Characteristics Of VANET

• High node mobility, solution scalability requirements and wide variety of environmental conditions are three of the most important challenges of these decentralized self-organizing networks. A particular problem that has to be faced comes from the high speeds of vehicles in some scenarios such as highways. These characteristics collude with most iterative algorithms intended to optimize the use of
the channel bandwidth or of predefined routes.

• Security and privacy requirements in VANET shave to be balanced. On the one hand, receivers want to make sure that they can trust the source of information but on the other hand, this might disagree with privacy requirements of the sender.

• The radio channel in VANET scenarios present critical features for developing wireless communications, which degrade strength and quality of signals.

• The need for standardization of VANET communications should allow flexibility as these networks have to operate with many different brands of equipment and vehicle manufacturers.

• Real-time communication is a necessary condition because no delay can exist in the transmission of safety-related information. This implies that VANET communication requires fast processing and exchange of information.

• The existence of a central registry of vehicles, possible periodic contact with it, and qualified mechanisms for the exigency of fulfilment of the law are three usual assumptions that are necessary for some proposed solutions.

- Communication for information exchange is based on node-to-node connections. This distributed nature of the network implies that nodes have to relay on other nodes to make decisions, for instance about route choice, and also that any node in a VANET can act either as a host requesting information or a router distributing data, depending on the circumstances.

Security issues in MANET

There are several general security requirements, such as authenticity, scalability, privacy, anonymity, cooperation, stability and low delay of communications, which must be considered in any wireless network, and which in VANETs are even more challenging because of their specific characteristics such as high mobility, no fixed infrastructure and frequently changing topology that range from rural road scenarios with little traffic to cities or highways with a huge number of communications. The lack of a centralized infrastructure in charge of synchronization and coordination of transmissions makes that one of the hardest tasks in the resulting decentralized and self-organizing VANETs is the management of the wireless channel to reach an efficient use of its bandwidth.

Security issues in MANET

- **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 owner RF Transmissions:**
  It is possible for a malicious node having high power RF transmission capability to continuously transmit and monopolies the medium and cause its neighbours nodes or the entire targeted MANET to wait endlessly for transmitting their messages.
- **Limited computational capabilities:**
  Nodes in an adhoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute intensive security solutions such as setting up a public key cryptosystems.
- **Limited power Supply:**
  Since nodes normally rely on battery power an attacker might attempt exhaust batteries by causing unnecessary transmissions to take lace pat the targeted node or might cause excessive computations to be carried out by the targeted nodes.

Attacks in MANET of various layers

- **Dropping attacks**: Here data packets that are transmitted are dropped at compromised or selfish
  node.
- **Modification attacks**: In this type of attack they alter the packets and disrupt the communication
- between the nodes in the network
- **Fabrication attacks**: Here the attacker node send fake message without getting any related message. and this can be called as forge reply.
- **Timing attacks**: Here attacker attack other nodes to it by advertising itself as node near to actual
  node Indicate that it is having a fresh shortest path to destination.

Network layer: Network layer contains the following attacks they are:

- **Black hole attack**: In this type of attack node advertises itself having shortest route to destination and thus attracts the data in the network.
- **Wormhole attack**: This type of attack makes a tunnel between two malicious nodes and attracts
  the data flow through these attacker nodes.
- **Internal Attacks**
  Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. B. External attacks.
- **External attacks**
- These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. . External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:
- **Passive attacks**
  MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network
  traffic or accumulates data from it.
- **Active Attacks**
  Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks
  can be carried out by outside sources that do not belong to the network.
- **Gray-Hole Attack**
  Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behavior:
- **Node dependent attack** – drops DATA packets destined towards a certain victim node or coming from certain node while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.
- **Time dependent attack** – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances.