Mobile IP, Dynamic Host Configuration Protocol, Routing in MANETs: DSDV, DSR, AODV and ZRP. MANETS vs VAN

Mobile IP

Need for Mobile IP:

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached**.** A host cannot change its IP address without terminating on-going sessions and restarting them after it acquires a new address. Other link layer mobility solutions exist but are not sufficient enough for the global Internet.

Mobility is the ability of a node to change its point-of-attachment while maintaining all existing communications and using the same IP address.

Nomadicity allows a node to move but it must terminate all existing communications and then can initiate new connections with a new address.

Mobile IP is a network layer solution for homogenous and heterogeneous mobility on the global Internet which is scalable, robust, secure and which allows nodes to maintain all ongoing communications while moving.

Design Goals: Mobile IP was developed as a means for transparently dealing with problems of mobile users. Mobile IP was designed to make the size and the frequency of required routing updates as small as possible. It was designed to make it simple to implement mobile node software. It was designed to avoid solutions that require mobile nodes to use multiple addresses.

Requirements: There are several requirements for Mobile IP to make it as a standard. Some of them are:

1. ***Compatibility*****:** The whole architecture of internet is very huge and a new standard cannot introduce changes to the applications or network protocols already in use. Mobile IP is to be integrated into the existing operating systems. Also, for routers also it may be possible to enhance its capabilities to support mobility instead of changing the routers which is highly impossible. Mobile IP must not require special media or MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does. Finally, end-systems enhanced with a mobile IP implementation should still be able to communicate with fixed systems without mobile IP.
2. ***Transparency*****:** Mobility remains invisible for many higher layer protocols and applications. Higher layers continue to work even if the mobile computer has changed its point of attachment to the network and even notice a lower bandwidth and some interruption in the service. As many of today's applications have not been designed to use in mobile environments, the effects of mobility will be higher delay and lower bandwidth.

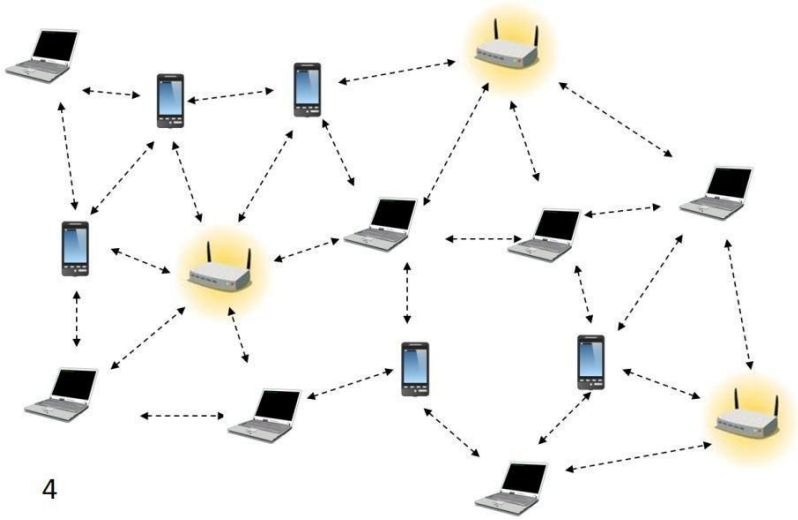
3. *Scalability and efficiency*: The efficiency of the network should not be affected even if a new mechanism is introduced into the internet. Enhancing IP for mobility must not generate many new messages flooding the whole network. Special care is necessary to be taken considering the lower bandwidth of wireless links. Many mobile systems have a wireless link to an attachment point. Therefore, only some additional packets must be necessary between a mobile system and a node in

the network. It is indispensable for a mobile IP to be scalable over a large number of participants in the whole internet, throughout the world.

4. ***Security*:** Mobility possesses many security problems. A minimum requirement is the authentication of all messages related to the management of mobile IP. It must be sure for the IP layer if it forwards a packet to a mobile host that this host really is the receiver of the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There is no way to prevent faked IP addresses and other attacks.

The goal of a mobile IP can be summarized as: 'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols'.

Mobile Ad hoc NETworks (MANETs) are wireless networks which are characterized by dynamic topologies and no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and, as much, may be required to forward packets between nodes which cannot directly communicate with one another. Each MANET node has much smaller frequency spectrum requirements that that for a node in a fixed infrastructure network. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.



4

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set upanywhere and anytime without using any pre-existing fixed network infrastructure.

MANET- Characteristics

- Dynamic network topology
- Bandwidth constraints and variable link capacity
- Energy constrained nodes
- Multi-hop communications

- Limited security
- Autonomous terminal
- Distributed operation
- Light-weight terminals

Need for Ad Hoc Networks

- Setting up of fixed access points and backbone infrastructure is not alwaysviable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)

Ad hoc networks:

- Do not need backbone infrastructure support
- Are easy to deploy
- Useful when infrastructure is absent, destroyed or impractical

Properties of MANETs

- MANET enables fast establishment of networks. When anew network is to be established, the only requirement is to provide a new set of nodes with limited wireless communication range. A node has limited capability, that is, it can connect only to the nodes which are nearby. Hence it consumes limited power.
- A MANET node has the ability to discover a neighboring node and service. Using a service discovery protocol, a node discovers the service of a nearby node and communicates to a remote node in the MANET.
- MANET nodes have peer-to-peer connectivity among themselves.
- MANET nodes have independent computational, switching (or routing), and communication capabilities.
- The wireless connectivity range in MANETs includes only nearest node connectivity.
- The failure of an intermediate node results in greater latency in communicating with the remote server.
- Limited bandwidth available between two intermediate nodes becomes a constraint for the MANET. The node may have limited power and thus computations need to be energy- efficient.
- There is no access-point requirement in MANET. Only selected access points are provided for connection to other networks or other MANETs.
- MANET nodes can be the iPods, Palm handheld computers, Smartphone‘s, PCs, smart labels, smart sensors, and automobile-embedded systems\
- MANET nodes can use different protocols, for example, IrDA,

Bluetooth, ZigBee, 802.11, GSM, and TCP/IP.MANET node performs data caching, saving, andaggregation.

- MANET mobile device nodes interact seamlessly when they move with the nearby wireless nodes, sensor nodes, and embedded devices in automobiles so that the seamless connectivity is maintained between the devices.

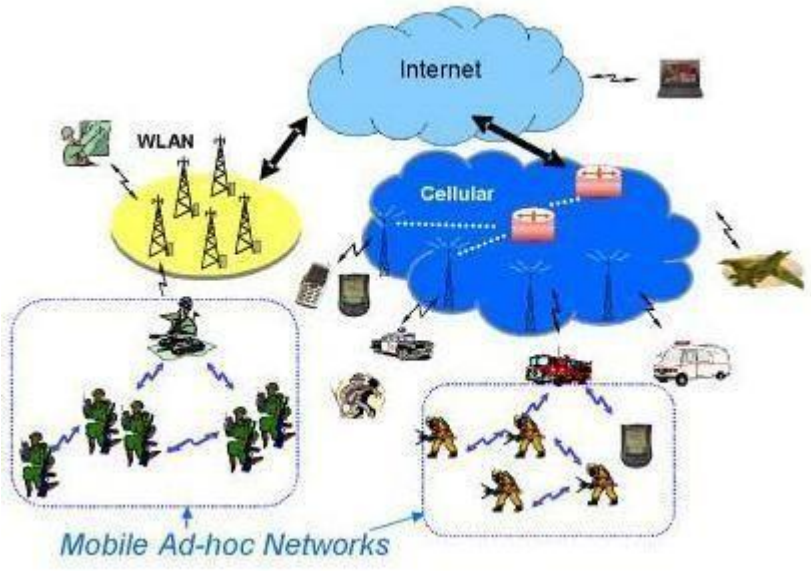
MANET challenges

To design a good wireless ad hoc network, various challenges have to be taken into account:

- *Dynamic Topology*: Nodes are free to move in an arbitrary fashion resulting in the topology changing arbitrarily. This characteristic demands dynamic configuration of the network.
- *Limited security*: Wireless networks are vulnerable to attack. Mobile ad hoc networks are more vulnerable as by design any node should be able to join or leave the network at any time. This requires flexibility and higher openness.
- *Limited Bandwidth*: Wireless networks in general are bandwidth limited. In an ad hoc network, it is all the more so because there is no backbone to handle or multiplex higher bandwidth
- *Routing*: Routing in a mobile ad hoc network is complex. This depends on many factors, including finding the routing path, selection of routers, topology, protocol etc.

Applications of MANETS

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. Some of the main application areas of MANET‘s are:



Military battlefield– soldiers, tanks, planes. Ad- hoc networking would allow the militaryto take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters.

Sensor networks – to monitor environmental conditions over a large area

Local level – Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

Personal Area Network (PAN) – pervasive computing i.e. to provide flexible connectivity between personal electronic devices or home appliances. Short-range MANET can simplify the intercommunication between various mobile devices (such as aPDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS.

Vehicular Ad hoc Networks – intelligent transportation i.e. to enable real time vehicle monitoring and adaptive traffic control

Civilian environments – taxi cab network, meeting rooms, sports stadiums, boats, small aircraft

Emergency operations – search and rescue, policing and fire fighting and to provide connectivity between distant devices where the network infrastructure is unavailable. Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non- existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held.

Routing in MANET's

Routing in Mobile Ad hoc networks is an important issue as these networks do not have fixed infrastructure and routing requires distributed and cooperative actions from all nodes in the network. MANET's provide point to point routing similar to Internet routing. The major difference between routing in MANET and regular internet is the route discovery mechanism. Internet routing protocols such as RIP or OSPF have relatively long converge times, which is acceptable for a wired network that has infrequent topology changes. However, a MANET has a rapid topology changes due to node mobility making the traditional internet routing protocols inappropriate. MANET-specific routing protocols have been proposed, that handle topology changes well, but they have large control overhead and are not scalable for large networks. Another major difference in the routing is the network address. In internet routing, the network address (IP address) is hierarchical containing a network ID and a computer ID on that network. In contrast, for most MANET's the network address is simply an ID of the node in the network and is not hierarchical. The routing protocol must use the entire address to decide the next hop.

Some of the fundamental differences between wired networks & ad-hoc networks are:

- Asymmetric links: - Routing information collected for one direction is of no use for the other direction. Many routing algorithms for wired networks rely on a symmetric scenario.
- Redundant links: - In wired networks, some redundancy is present to survive link failures and this redundancy is controlled by a network administrator. In ad-hoc networks, nobody controls redundancy resulting in many redundant links up to the extreme of a complete meshed topology.
- Interference: - In wired networks, links exist only where a wire exists, and connections are planned by network administrators. But, in ad-hoc networks links come and go depending on transmission characteristics, one transmission might interfere with another and nodes might overhear the transmission of other nodes.
- Dynamic topology: - The mobile nodes might move in an arbitrary manner or medium characteristics might change. This result in frequent changes in topology, so snapshots are valid only for a very short period of time. So, in ad-hoc networks, routing tables must somehow reflect these frequent changes in topology and routing algorithms have to be adopted.

Summary of the difficulties faced for routing in ad-hoc networks

- Traditional routing algorithms known from wired networks will not work efficiently or fail completely. These algorithms have not been designed with a highly dynamic topology, asymmetric links,

or interference in mind.

- Routing in wireless ad-hoc networks cannot rely on layer three knowledge alone. Information from lower layers concerning connectivity or interference can help routing algorithms to find a good path.
- Centralized approaches will not really work, because it takes too long to collect the current status and disseminate it again. Within this time the topology has already changed.
- Many nodes need routing capabilities. While there might be some without, at least one router has to be within the range of each node. Algorithms have to consider the limited battery power of these nodes.
- The notion of a connection with certain characteristics cannot work properly. Ad-hoc networks will be connectionless, because it is not possible to maintain a connection in a fast changing environment and to forward data following this connection. Nodes have to make local decisions for forwarding and send packets roughly toward the final destination.
- A last alternative to forward a packet across an unknown topology is flooding. This approach always works if the load is low, but it is very inefficient. A hop counter is needed in each packet to avoid looping, and the diameter of the ad-hoc network.

Types of MANET Routing Algorithms:

1. Based on the information used to build routing tables :
   - *Shortest distance algorithms*: algorithms that use distance information to build routingtables.
   - *Link state algorithms*: algorithms that use connectivity information to build a topologygraph that is used to build routing tables.

2. Based on when routing tables are built:
   - *Proactive algorithms*: maintain routes to destinations even if they are not needed. Someof the examples are Destination Sequenced Distance Vector (DSDV), Wireless Routing Algorithm (WRP), Global State Routing (GSR), Source-tree Adaptive Routing (STAR), Cluster-Head Gateway Switch Routing (CGSR), Topology Broadcast Reverse Path Forwarding (TBRPF), Optimized Link State Routing (OLSR) etc.
     - ❖ Always maintain routes:- Little or no delay for route determination
     - ❖ Consume bandwidth to keep routes up-to-date
     - ❖ Maintain routes which may never be used
     - ❖ Advantages: low route latency, State information,

QoS guarantee related toconnection set-up or other real-time requirements

- ❖ Disadvantages: high overhead (periodic updates) and route repair dependson update frequency

- *Reactive algorithms*: maintain routes to destinations only when they are needed. Examples are Dynamic Source Routing (DSR), Ad hoc-On demand distance Vector (AODV), Temporally ordered Routing Algorithm (TORA), Associativity-Based Routing (ABR) etc
  - ❖ only obtain route information when needed
  - ❖ Advantages: no overhead from periodic update, scalability as long as there isonly light traffic and low mobility.
  - ❖ Disadvantages: high route latency, route caching can reduce latency
- *Hybrid algorithms*: maintain routes to nearby nodes even if they are not needed and maintain routes to far away nodes only when needed. Example is Zone Routing Protocol (ZRP).

Which approach achieves a better trade-off depends on the traffic and mobility patterns.

Destination sequence distance vector (DSDV)

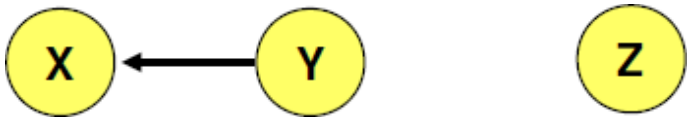
Destination sequence distance vector (DSDV) routing is an example of proactive algorithms and an enhancement to distance vector routing for ad-hoc networks. Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes 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. The strategies to avoid this problem which are used in fixed networks 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 adds the concept of sequence numbers to the distance vector algorithm. 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.

Each node maintains a routing table which stores next hop, cost metric towards each destination and a sequence number that is created by the destination itself. Each node periodically forwards routing table to

neighbors. Each node increments and appends its sequence number when sending its local routing table. Each route is tagged with a sequence number; routes with greater sequence numbers are preferred. Each node advertises a monotonically increasing even sequence number for itself. When a node decides that a route is broken, it increments the sequence number of the route and advertises it with infinite metric. Destination advertises new sequence number.

When X receives information from Y about a route to Z,



- Let destination sequence number for Z at X be S(X), S(Y) is sent from Y
- If S(X) > S(Y), then X ignores the routing information received from Y
- If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then Xsets Y as the next hop to Z
- If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y)

Besides being loop-free at all times, DSDV has low memory requirements and a quick convergence via triggered updates. Disadvantages of DSDV are, large routing overhead, usage of only bidirectional links and suffers from count to infinity problem.

Dynamic Source Routing

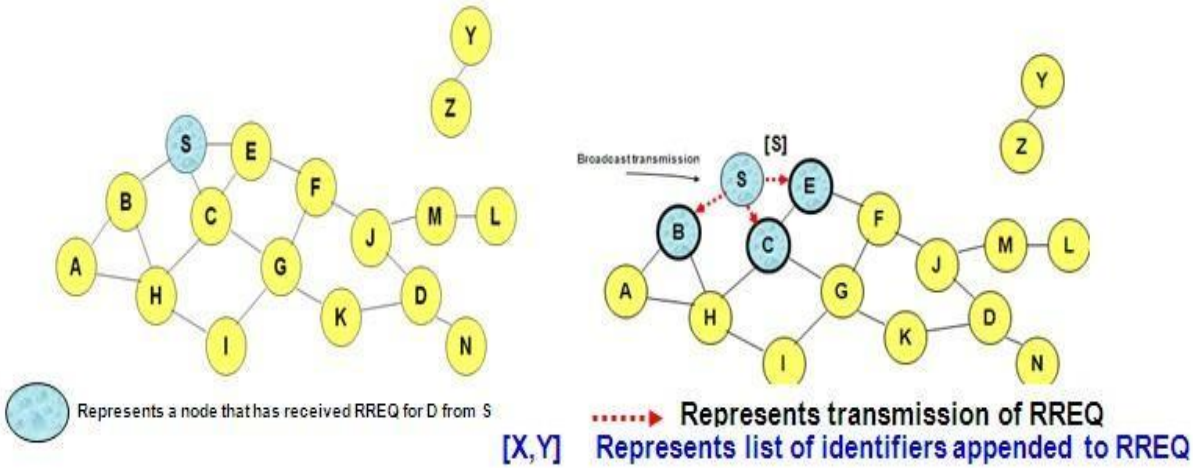
The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use.

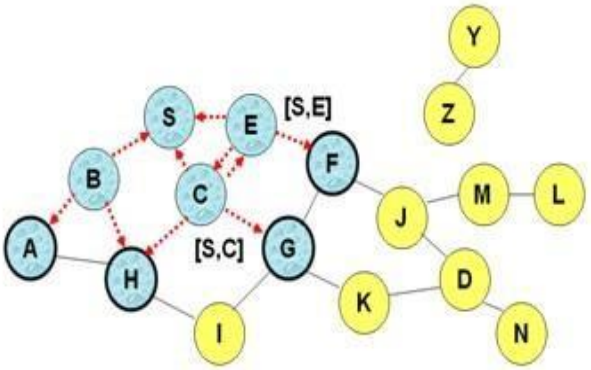
Route discovery. If the source does not have a route to the destination in its route cache, it broadcasts a route request (RREQ) message specifying the destination node for which the route is requested. The RREQ message includes a route record which specifies the sequence of nodes traversed by the message. When an intermediate node receives a RREQ, it checks to see if it is already in the route record. If it is, it drops the

message. This is done to prevent routing loops. If the intermediate node had received the RREQ before, then it also drops the message. The intermediate node forwards the RREQ to the next hop according to the route specified in the header. When the destination receives the RREQ, it sends back a route reply message. If the destination has a route to the source in its route cache, then it can send a route response (RREP) message along this route. Otherwise, the RREP message can be sent along the reverse route back to the source. Intermediate nodes may also use their route cache to reply to RREQs. If an intermediate node has a route to the destination in its cache, then it can append the route to the route record in the RREQ, and send an RREP back to the source containing this route. This can help limit flooding of the RREQ. However, if the cached route is out-of-date, it can result in the source receiving stale routes.

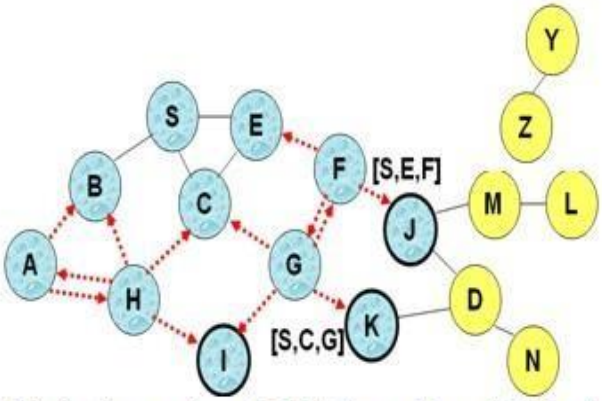
Route maintenance. When a node detects a broken link while trying to forward a packet to the next hop, it sends a route error (RERR) message back to the source containing the link in error. When an RERR message is received, all routes containing the link in error are deleted at that node.

As an example, consider the following MANET, where a node S wants to send a packet to D, but does not know the route to D. So, it initiates a route discovery. Source node S floods Route Request (RREQ). Each node appends its own identifier when forwarding RREQ as shown below.

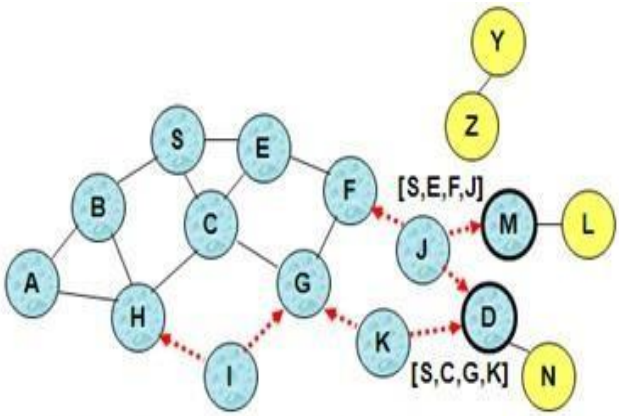




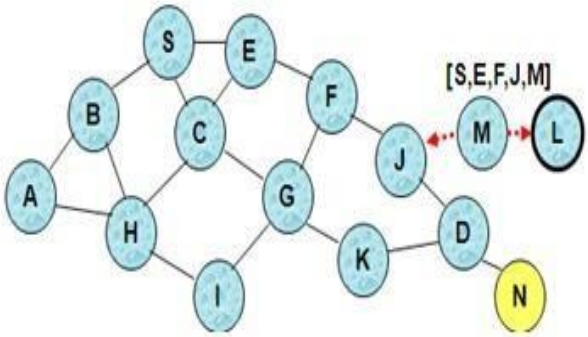
Node H receives packet RREQ from two neighbors: potential for collision



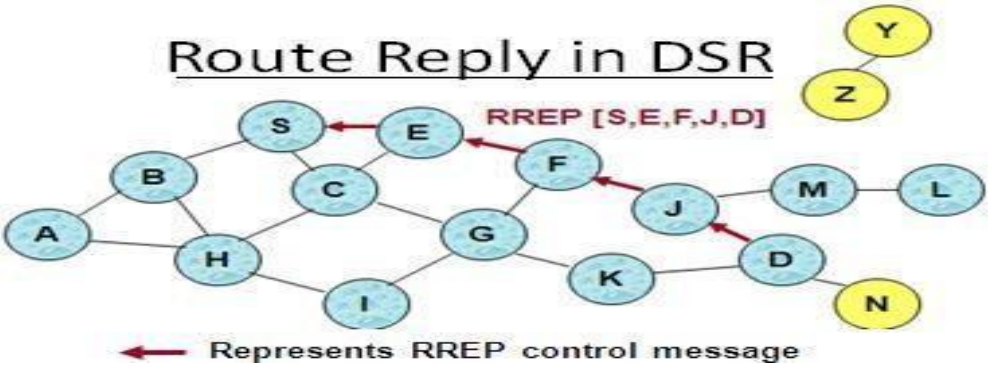
Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide



Node D does not forward RREQ, because node D is the intended target of the route discovery

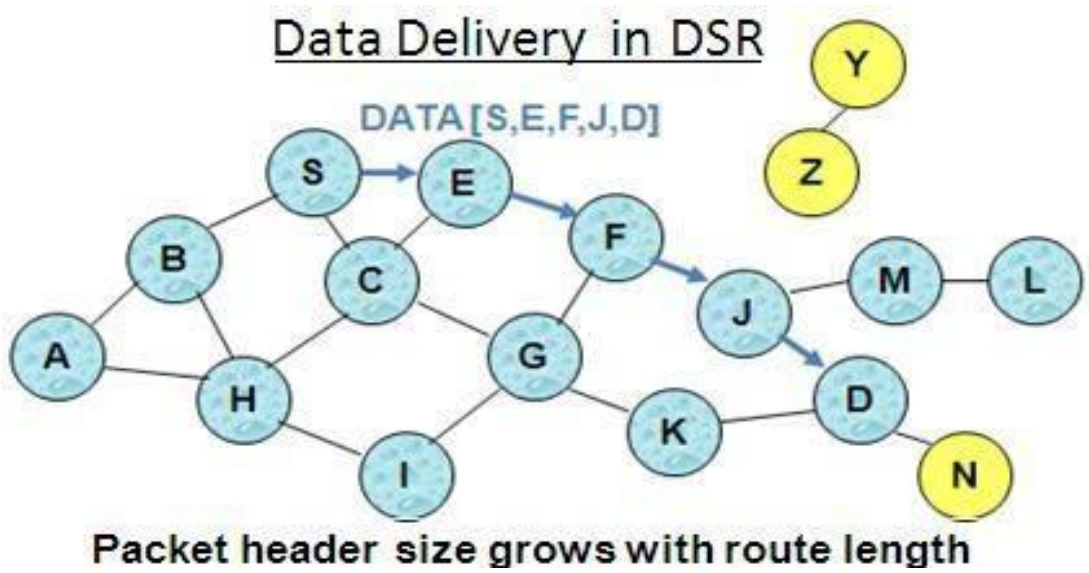


Destination D on receiving the first RREQ, sends a Route Reply (RREP). RREP is sent on a route obtained by reversing the route appended to received RREQ. RREP includes the route fromS to D on which RREQ was received by node D.

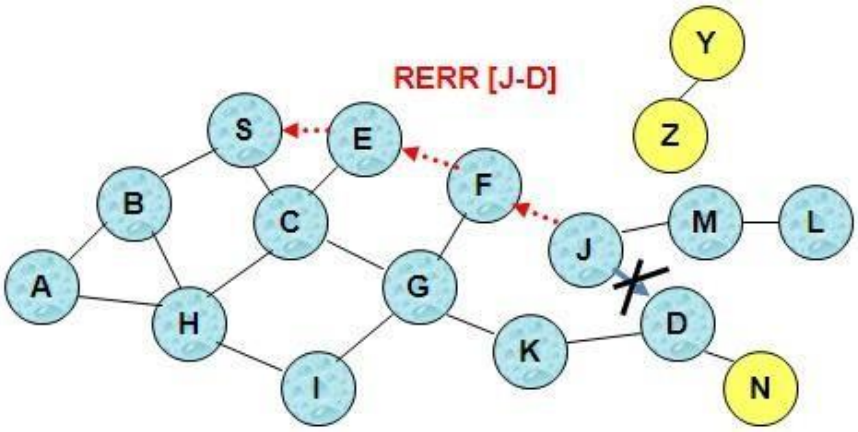
Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional. If Unidirectional (asymmetric) links are allowed, then RREP may need a

route discovery from S to D. Node S on receiving RREP, caches the route included in the RREP. When node S sends a data packet to D, the entire route is included in the packet header

{hence the name source routing}. Intermediate nodes use the source route included in a packet todetermine to whom a packet should be forwarded.



J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails. Nodes hearing RERR update their route cache to remove link J- D



Advantages of DSR:

- Routes maintained only between nodes who need to communicate-- reduces overhead ofroute maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediatenodes replying from local caches

Disadvantages of DSR:

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes -- insertion of random delays before forwarding RREQ
- Increased contention if too many route replies come back due to nodes replying using their local cache-- Route Reply *Storm* problem. Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route
- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches

An optimization for DSR can be done called as Route Caching. Each node caches a new route it learns by *any means.* In the above example, When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F. When node K receives Route Request [S,C,G] destined for node, node K learns route [K,G,C,S] to node S. When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D. When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D. A node may also learn a route when it overhears Data packets. Usage of Route cache can speed up route discovery and can also reduce propagation of route Requests. The disadvantages are, stale caches can adversely affect performance. With passage oftime and host mobility, cached routes may become invalid.

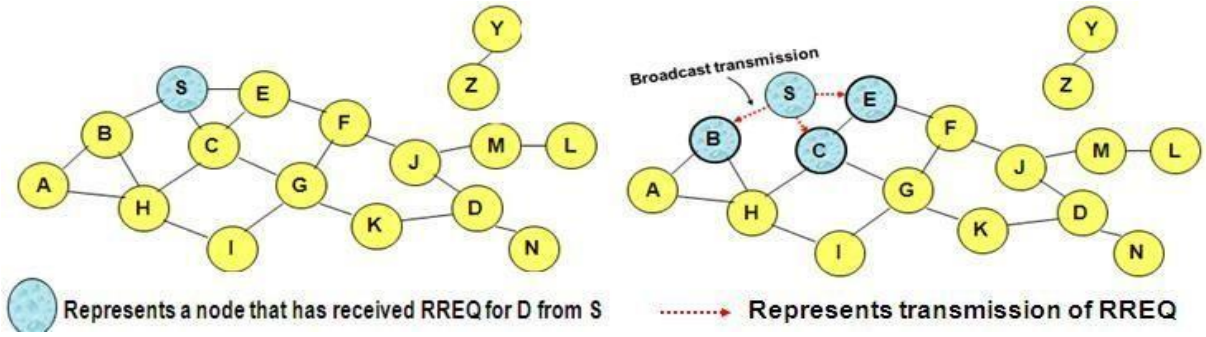
Ad Hoc On-Demand Distance Vector Routing (AODV)

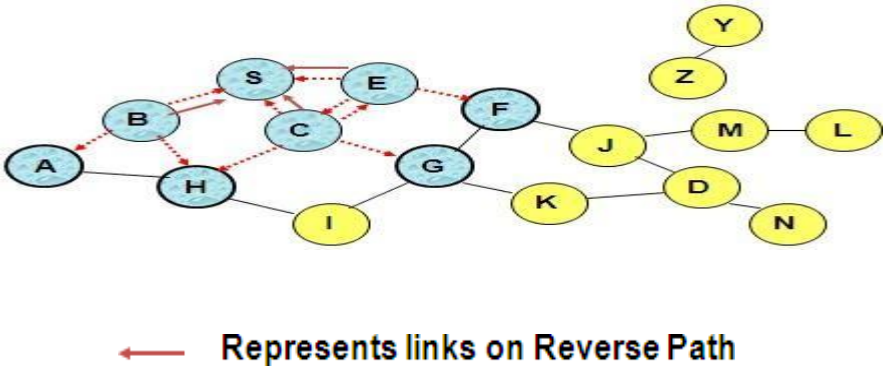
AODV is another reactive protocol as it reacts to changes and maintains only the active routes in the caches or tables for a pre-specified expiration time. Distance vector means a set of distant nodes, which defines the path to destination. AODV can be considered as a descendant of DSR and DSDV algorithms. It uses the same route discovery mechanism used by DSR. DSR includes source routes in packet headers and resulting large headers can sometimes degrade performance, particularly when data contents of a packet are small. AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes. AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate. However, as opposed to DSR, which uses source routing, AODV uses hop-by-hop routing by maintaining routing table entries at intermediate nodes.

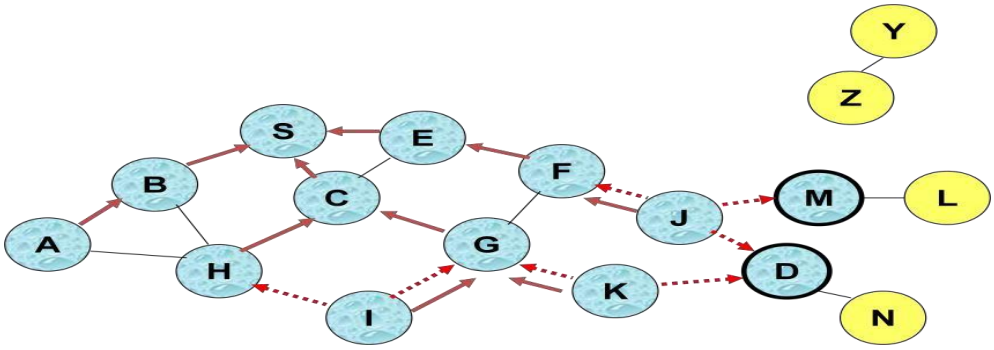
Route Discovery. The route discovery process is initiated when a source needs a route to a destination and it does not have a route in its routing table. To initiate route discovery, the source floods the network with a

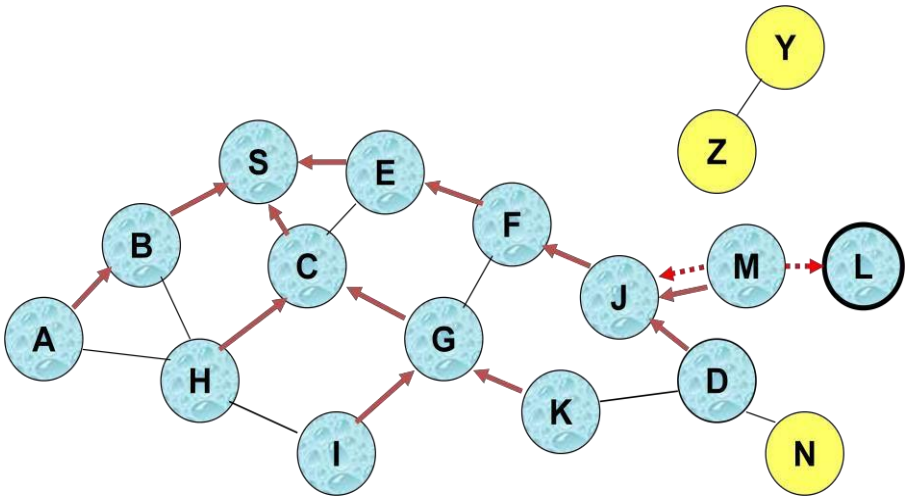
RREQ packet specifying the destination for which the route is requested. When a node receives an RREQ packet, it checks to see whether it is the destination or whether it has a route to the destination. If either case is true, the node generates an RREP packet, which is sent back to the source along the reverse path. Each node along the reverse path sets up a forward pointer to the node it received the RREP from. This sets up a forward path from the source to the destination. If the node is not the destination and does not have a route to the destination, it rebroadcasts the RREQ packet. At intermediate nodes duplicate RREQ packets are discarded. When the source node receives the first RREP, it can begin sendingdata to the destination. To determine the relative degree out-of-datedness of routes, each entry in the node routing table and all RREQ and RREP packets are tagged with a destination sequence number. A larger destination sequence number indicates a more current (or more recent) route. Upon receiving an RREQ or RREP packet, a node updates its routing information to set up the reverse or forward path, respectively, only if the route contained in the RREQ or RREP packet is more current than its own route.

Route Maintenance. When a node detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process. Routes are also deleted from the routing table if they are unused for a certain amount of time.

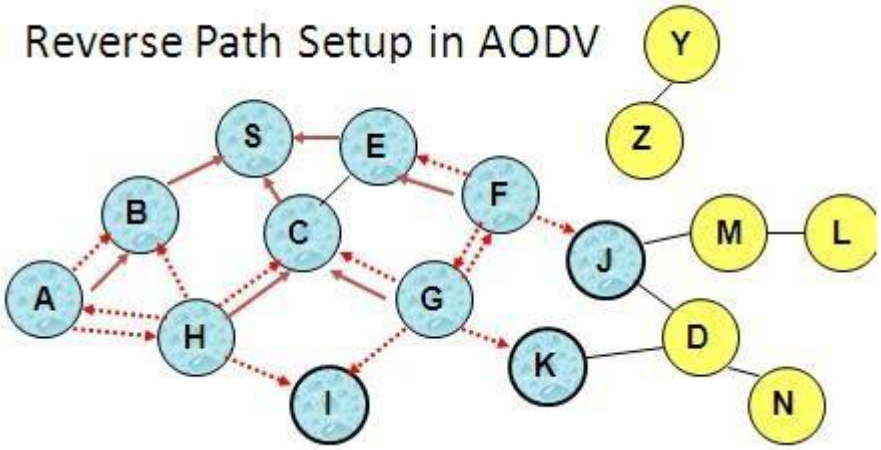




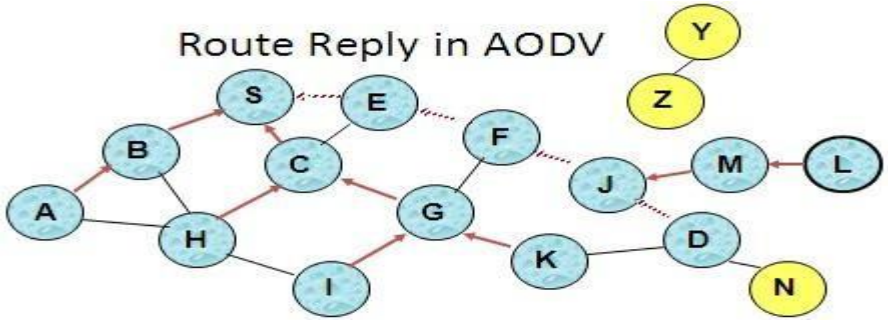




Node D does not forward RREQ, because node D is the intended target of the RREQ



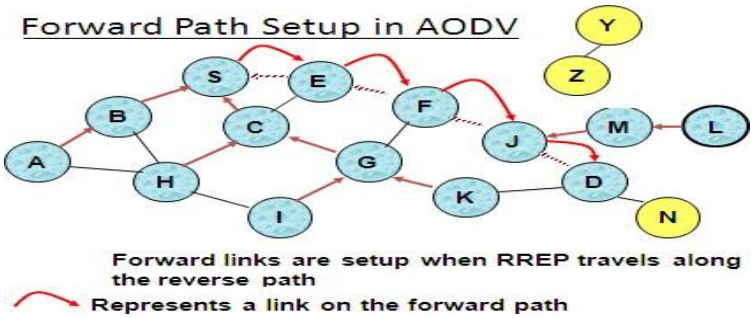
Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

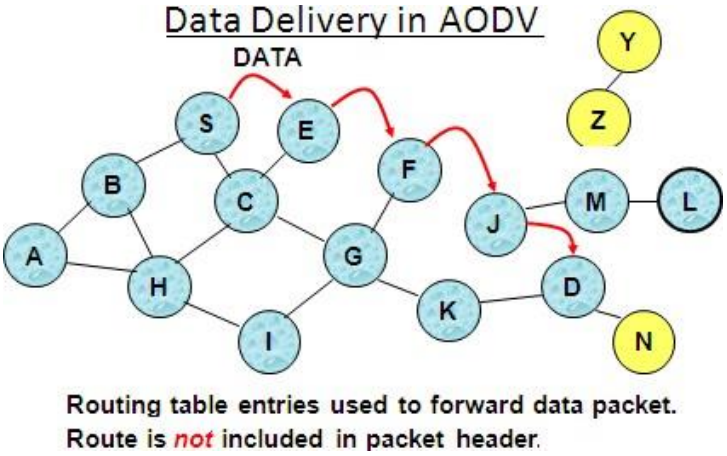


Represents links on path taken by RREP

An intermediate node (not the destination) may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S. To determine whether the path known to an intermediate node is more recent, *destination sequence numbers* are used. The likelihood that an intermediate node will send a Route Reply when using AODV is not as high as DSR. A new Route Request by node S for a destination is assigned a higher destination sequence

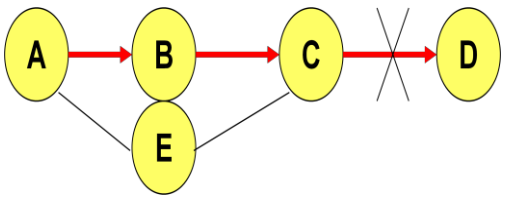
number. An intermediate node which knows a route, but with a smaller sequence number, cannot send Route Reply





When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generatesa RERR message Node X increments the destination sequence number for D cached at node
X. The incremented sequence number *N* is included in the RERR. When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as
N. When node D receives the route request with destination sequence number N, node D willset its sequence number to N, unless it is already larger than N.

Sequence numbers are used in AODV to avoid using old/broken routes and to determine whichroute is newer. Also, it prevents formation of loops.



Assume that A does not know about failure of link C-D becauseRERR sent by C is lost.

Now C performs a route discovery for D. Node A receives theRREQ (say, via path C-E-A)

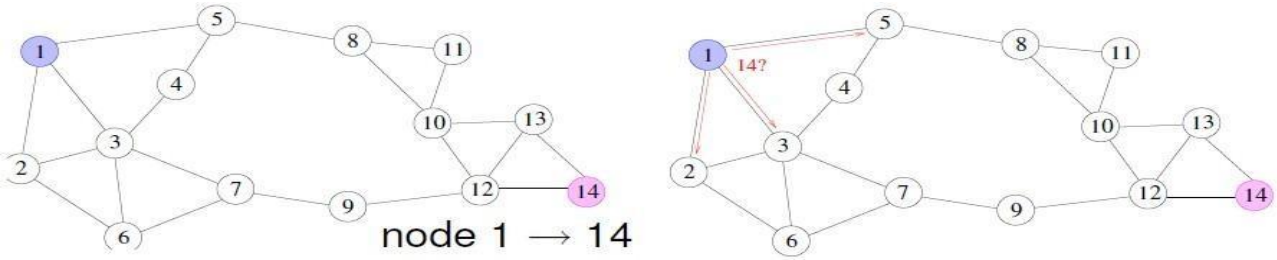
Node A will reply since A knows a route to D via node B resulting

in a loop (for instance, C-E-A-B-C)

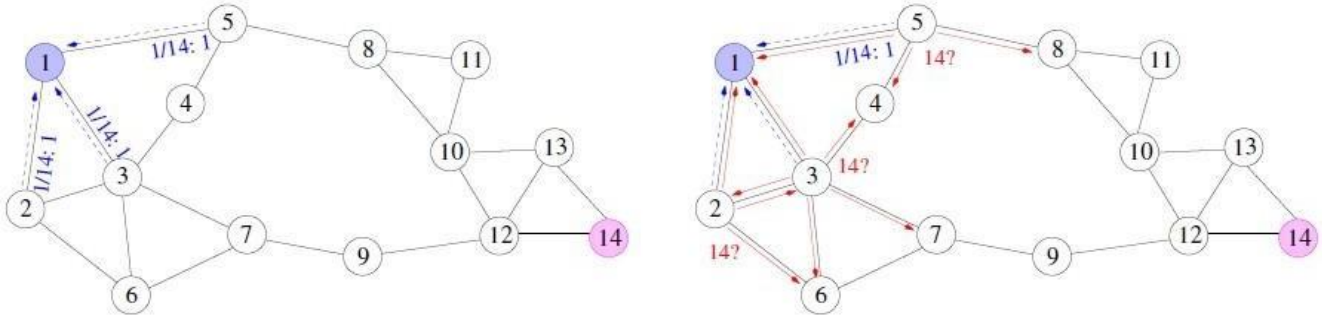
Neighboring nodes periodically exchange hello message and absence of hello message indicates a link failure. When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a **RERR message**. Node X increments the destination sequence number for D cached at node X. The incremented sequence number *N* is included in the RERR. When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as *N*. When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N.

Another example for AODV protocol:

Assume node-1 want to send a msg to node-14 and does not know the route. So, it broadcasts (floods) route request message, shown in red.

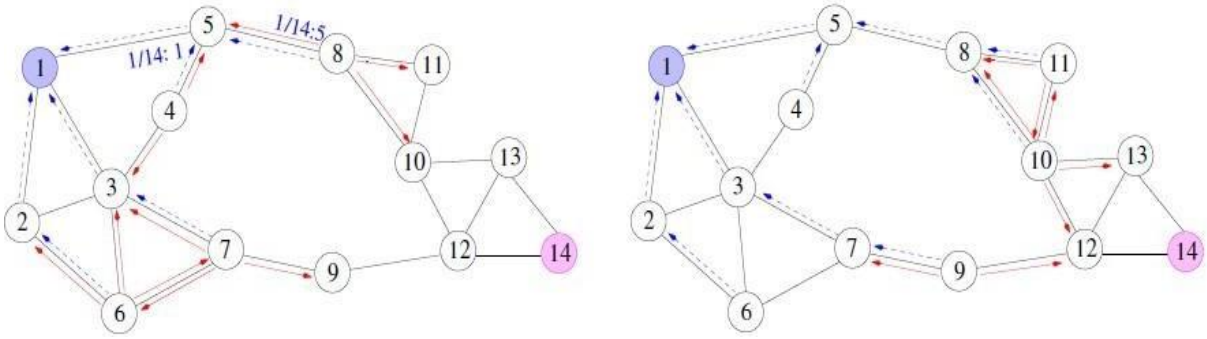


Node from which RREQ was received defines a reverse route to the source. (reverse routing table entries shown in blue).

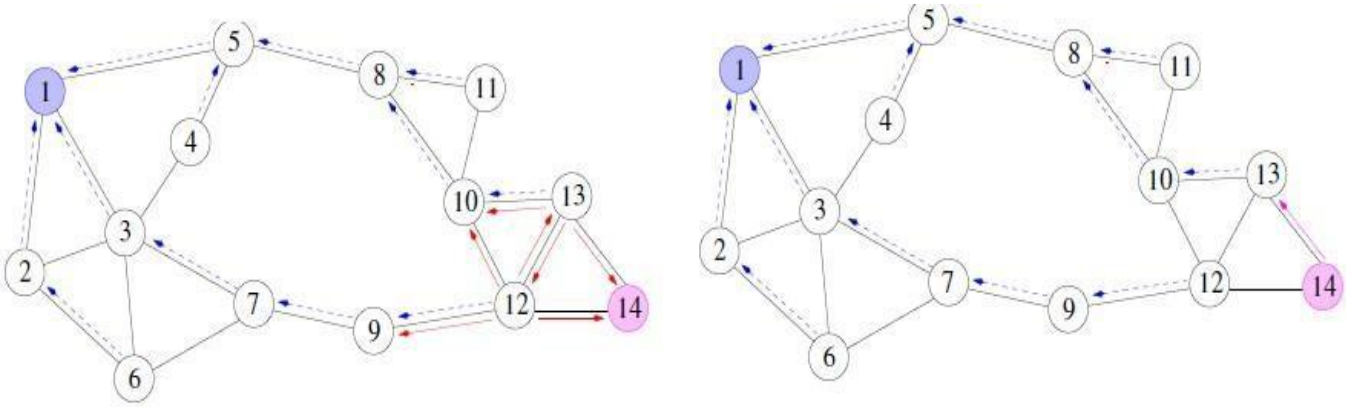


The route request is flooded through the network. Destination managed sequence number, ID prevent looping. Also, flooding is expensive and

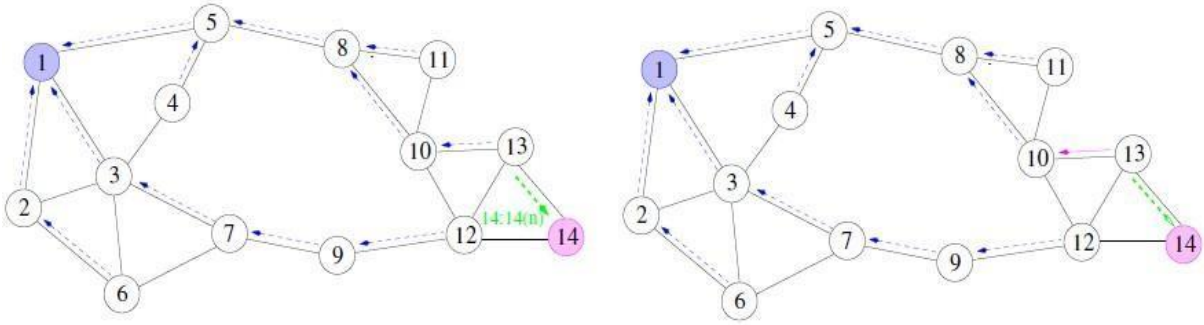
creates broadcast collision problem.



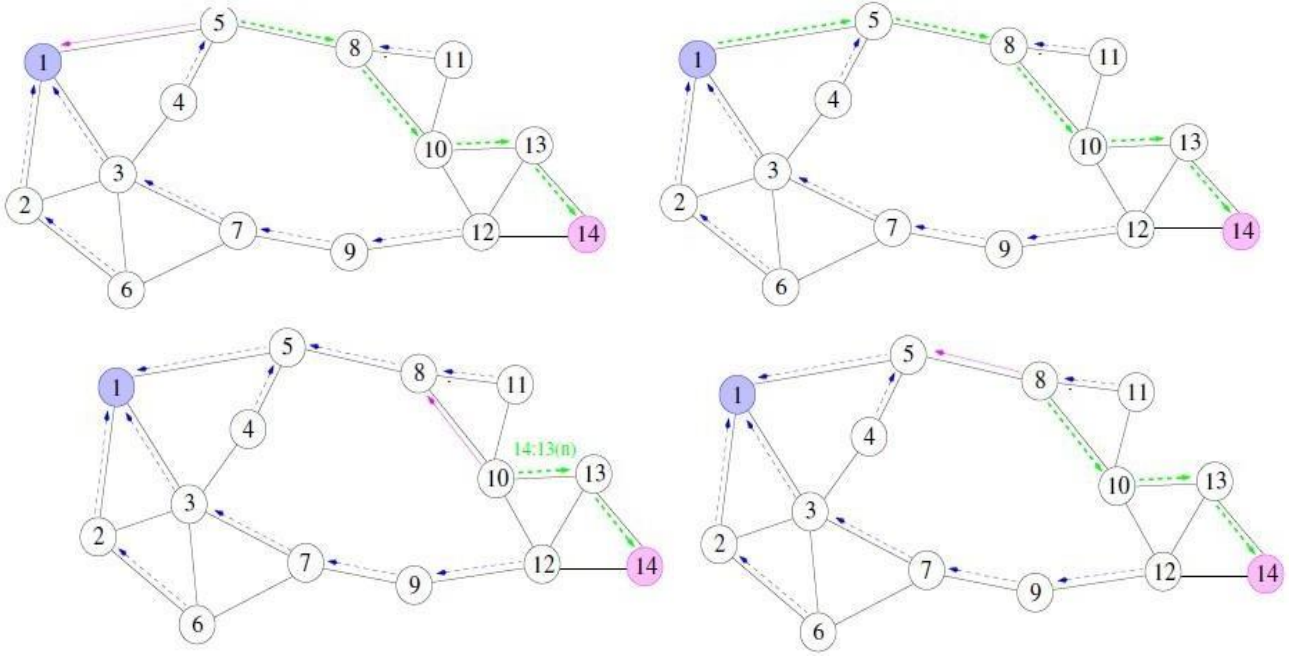
Route request arrives at the destination node-14. Upon receiving, destination sends route reply bysetting a sequence number(shown in pink)



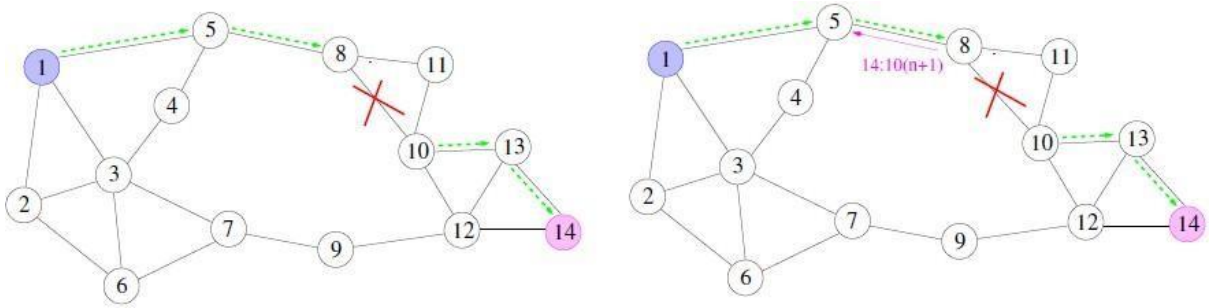
Routing table now contains forward route to the destination. Route reply follows reverse routeback to the source.



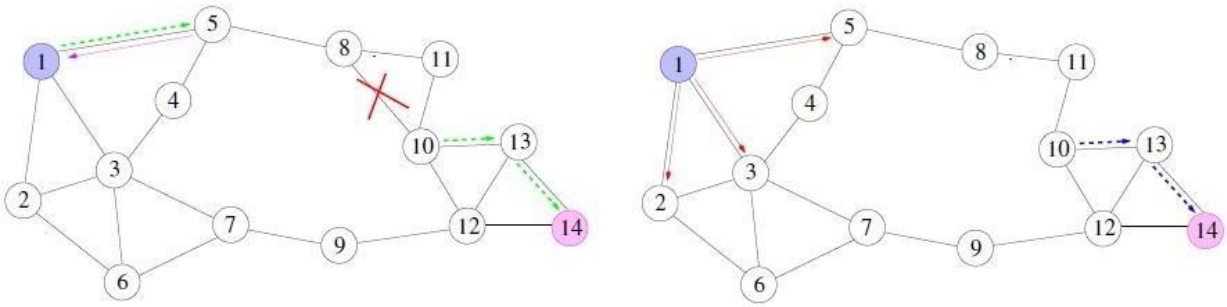
The route reply sets the forward table entries on its way back to the source. Once the route reply reaches the source, it adopts the destination sequence number. Traffic flows along the forward route. Forward route is refreshed and the reverse routes get timedout.



Suppose there has been a failure in one of the links. The node sends a return error message to thesource with incrementing the sequence number.



Once the source receives the route error, it re-initiates the route discoveryprocess.



A routing table entry maintaining a reverse path is purged after a timeout interval. Timeout should be long enough to allow RREP to come back. A routing table entry maintaining a forwardpath is purged if *not used* for a *active_route_timeout* interval. If no data is being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid).

Hierarchal State Routing (HSR)

A hierarchal link state routing protocol that solves the location management problem found in MMWN by using the logical subnets. A logical subnet is : a group of nodes that have common characteristics (e.g.

the subnet of students, the subnet of profs , employees etc.). Nodes of the same subnet do not have to be close to each other in the physicaldistance.

HSR procedure:

1. Based on the physical distance, nodes are grouped into clusters that are supervised by cluster-heads. There are more than one level of clustering.
2. Every node has two addresses :
   I. a hierarchal-ID ,(HID), composed of the node‘s MAC address prefixed by theIDs of its parent clusters.
   II. a logical address in the form <subnet,host>.
3. Every logical subnet has a home agent, i.e. a node that keeps track of the HID of all members of that subnet.
4. The HIDs of the home agents are known to all the cluster-heads, and the cluster-head can translate the subnet part of the node‘s logical address to the HID of the corresponding home agent.
5. when a node moves to a new cluster, the head of the cluster detects it and informs the node‘s home agents about node‘s new HID.
6. When a home agent moves to a new cluster, the head of the cluster detects it and informs all other cluster-heads about the home agent‘s new HID.

To start a session:

1. The source node informs its cluster-head about the logical address of the destination node.
2. The cluster-head looks up the HID of the destination node‘s home agent and uses it tosend query to the home agent asking about the destination's HID
3. After knowing the destination‘s HID, the cluster-head uses its topology map to find aroute to the destination‘s cluster-head.

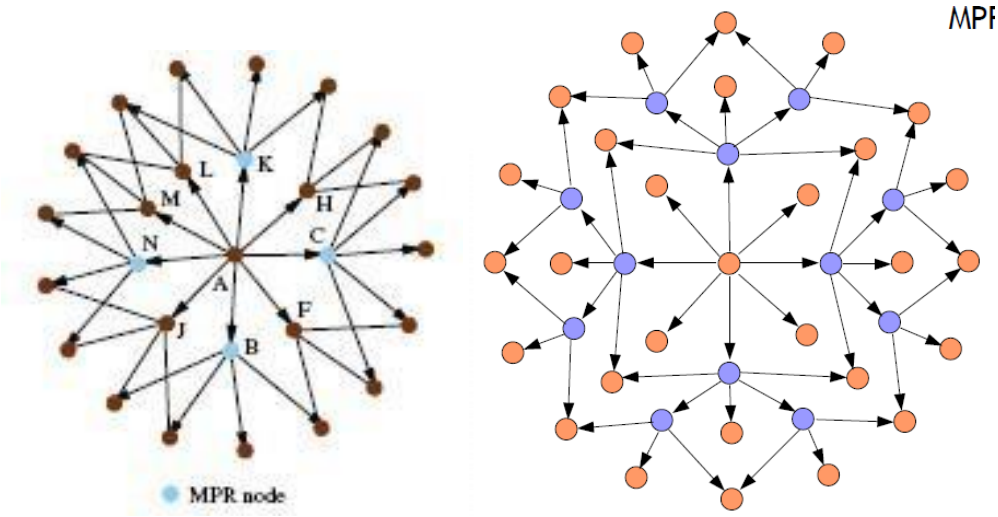
Disadvantages: cluster formation and maintenance.

Optimized Link State Routing Protocol

Optimized link state routing protocol (OLSR) has characteristics similar to those of link state flat routing table driven protocol, but in this case, only required updates are sent to the routing database. This reduces the overhead control packet size and numbers.

OSLR uses controlled flood to disseminate the link state information of each node.

- Every node creates a list of its one hop neighbors.
- Neighbor nodes exchange their lists with each other.
- Based on the received lists, each node creates its MPR.



The multipoint relays of each node, (MPR), is the minimal set of 1-hop nodes that covers all 2- hop points.

- The members of the MPR are the only nodes that can retransmit the link state information inan attempt to limit the flood.

Security in MANET's

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable

to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

1. External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

- **Denial of Service attack**: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.
- **Impersonation**: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can

also send fake routing packets, and gain access to some confidential information.

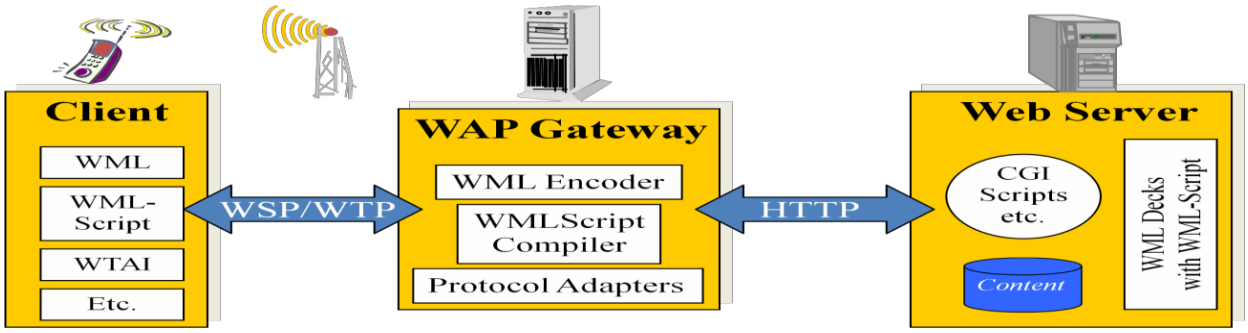
- **Eavesdropping:** This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.
- **Routing Attacks:** The malicious node makes routing services a target because it‘s an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.
- **Black hole Attack:**: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.
- **Wormhole Attack:** In a wormhole attack, an attacker receives packets at one point in the network, ―tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

- **Man- in- the- middle attack:** An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender~~ to communicate with receiver or impersonate the receiver to reply to the send~~er.

Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray-hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.



Vehicular Ad Hoc Networks (VANET) :

VANET is similar to MANET in terms, that is also do not need any infrastructure for data transmission. VANET play important role in aspect of safe driving, intelligent navigation, emergency and entertainment applications .It can be defined as an intelligent component of transport system as vehicle are able to communicate with each other as well as roadside base station, which are located at critical points of the road. Example :-Intersection and Construction Sites.

Difference between MANET and VANET :

S.No.	MANET	VANET
1	Production cost of MANET is cheap as compared to VANET	Much Expensive
2	Mobility of MANET is low as it make bit difficult for network enables the serving networks to locate a mobile subscriber's point.	High Mobility, as serving networks to locate a mobile subscriber's point is easy.
3	Change in network topology orientation is slow.	Frequent and very fast change of network topology,
4	Sparse node density.	Node density is frequent variables.
5	MANET HAVE 100 Kps bandwidth available.	VANET bandwidth is 1000 Kps.
6	It ranges Upto 100 m.	500 m range available in VANET.
7	MANET node lifetime depends on power resources.	Depend on lifetime vehicle.
8	MANET have medium reliability.	High reliability of VANET.
9	Movement of the nodes affects the operation of a MANET as node movement MANETs need to rely	Regular, moving pattern of nodes.

S.No.	MANET	VANET
	on robust routing protocols.And this MANET have random node movement.	
10	Attribute Based addressing scheme.	Location Bases addressing scheme.
11	Position acquisition is obtained using Ultrasonic.	VANET maintain position acquisition by using GPS, RADAR.
12	Availability of Multi-hop Routing	Weakly available Multi-hop Routing.