MODULE -2

ROUTING PROTOCOLS IN AD-HOC WIRELESS NWTWORKS

ISSUES IN DESIGNING A ROUTING PROTOCOL FOR AD HOC WIRELESS NETWORKS

The major challenges that a routing protocol designed for ad hoc wireless networks faces are:

Mobility

- Network topology is highly dynamic due to movement of nodes. hence, an ongoing session suffers frequent path breaks.
- Disruption occurs due to the movement of either intermediate nodes in the path or end nodes.
- Wired network routing protocols cannot be used in adhoc wireless networks because the nodes are here are not stationary and the convergence is very slow in wired networks.
- Mobility of nodes results in frequently changing network topologies
- Routing protocols for ad hoc wireless networks must be able to perform efficient and effective mobility management.

Bandwidth Constraint

- Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies.
- In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.
- This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.
- The limited bandwidth availability also imposes a constraint on routng protocols in maintaining the topological information.

Error-prone shared broadcast radio channel

- The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.
- The wireless links have time-varying characteristics in terms of link capacity and link-error probability.
- This requires that the adhoc wireless network routing protocol interact with the MAC layer to find alternate routes through better-quality links.
- Transmissions in ad hoc wireless networks result in collisions of data and control packets.
- Therefore, it is required that ad hoc wireless network routing protocols find paths with less congestion.

Hidden and exposed terminal problems

- The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the receiver, but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.
- Ex: consider figure 7.1. Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.

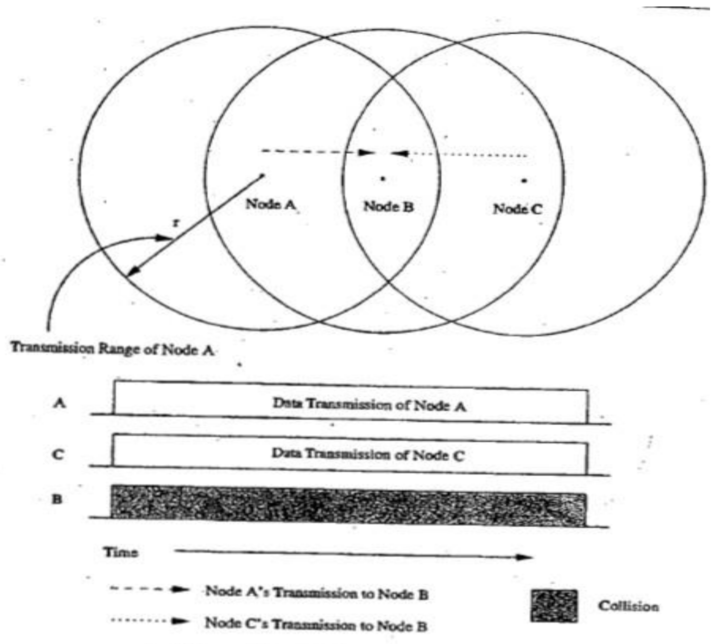


Figure 7.1. Hidden terminal problem.

- Solution for this problem include medium access collision avoidance (MACA):
  - Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two-way handshake control protocol called RTS-CTS protocol exchange.
  - This may not solve the problem completely but it reduces the probability of collisions.
- Medium access collision avoidance for wireless (MACAW):
  - An improved version of MACA protocol.
  - Introduced to increase the efficiency.
  - Requires that a receiver acknowledges each successful reception of data packet.
- Successful transmission is a four-way exchange mechanism, RTS-CTS-Data-ACK, as illustrated in figure 2.1.

- Other solutions include floor acquisition multiple access (FAMA) and Dual busy tone multiple access (DBTMA).
- The exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node to transmit to another node.
- Ex: consider the figure 7.3. Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

Resource Constraints

- Two essential and limited resources are battery life and processing power.
- Devices used in adhoc wireless networks require portability, and hence they also have size and weight constraints along with the restrictions on the power source.
- Increasing the battery power and processing ability makes the nodes bulky and less portable.

Characteristics of an Ideal Routing Protocol for ad hoc wireless networks

A routing protocol for ad hoc wireless networks should have the following characteristics:

- It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.
- It must be adaptive to frequent topology changes caused by the mobility of nodes.
- Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.
- It must be localized, as global state maintenance involves a huge state propagation control overhead.
- It must be loop-free and free from state routes.
- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.
- It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.
- It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.

- Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.
- It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

CLASSIFICATIONS OF ROUTING PROTOCOLS

A classification tree is shown below:

The routing protocol for adhoc wireless networks can be broadly classified into 4 categories based on

- Routing information update mechanism.
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources.

Based on the routing information update mechanism

Ad hoc wireless network routing protocols can be classified into 3 major categories based on the routing information update mechanism. They are:

- *Proactive or table-driven routing protocols* :
    - Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
    - Routing information is generally flooded in the whole network.
    - Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.
- *Reactive or on-demand routing protocols*:
    - Do not maintain the network topology information.
    - Obtain the necessary path when it is required, by using a connection establishment process.
- *Hybrid routing protocols:*
    - Combine the best features of the above two categories.
    - Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node.
    - For routing within this zone, a table-driven approach is used.
    - For nodes that are located beyond this zone, an on-demand approach is used.

Based on the use of temporal information for routing

The protocols that fall under this category can be further classified into two types :

- *Routing protocols using past temporal information:*
    - Use information about the past status of the links or the status of links at the time of routing to make routing decisions.
- *Routing protocols that use future temporal information:*
    - Use information about the about the expected future status of the wireless links to make approximate routing decisions.
    - Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

Based on the routing topology

Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

- *Flat topology routing protocols:*
    - Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.
    - It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.
- *Hierarchical topology routing protocols:*
    - Make use of a logical hierarchy in the network and an associated addressing scheme.
    - The hierarchy could be based on geographical information or it could be based on hop distance.

Based on the utilization of specific resources

- *Power-aware routing:*
  - Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.
  - The routing decisions are based on minimizing the power consumption either logically or globally in the network.
- *Geographical information assisted routing :*
  - Improves the performance of routing and reduces the control overhead by effectively utilizing the geographical information available.

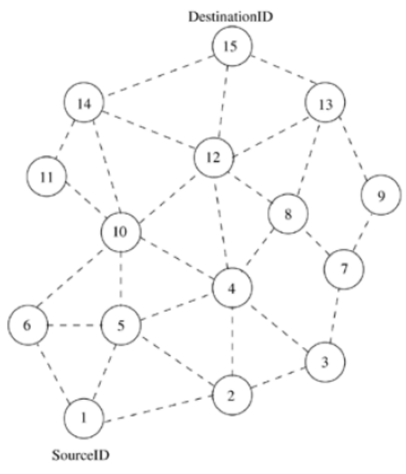
TABLE-DRIVEN ROUTING PROTOCOLS

- These protocols are extensions of the wired network routing protocols
- They maintain the global topology information in the form of tables at every node.
- Tables are updated frequently in order to maintain consistent and accurate network state information
- Ex: Destination sequenced distance vector routing protocol (DSDV), wireless routing protocol (WRP), source-tree adaptive routing protocol (STAR) and cluster-head gateway switch routing protocol (CGSR).

Destination sequenced distance-vector routing protocol (DSDV)

- It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network.
- It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence.
- As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times.
- The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology.
- The table updates are of two types:
  - ***Incremental updates:*** Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology.
  - ***Full dumps:*** Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU.
- Table updates are initiated by a destination with a new sequence number which is always greater than the previous one.

- Consider the example as shown in figure 2.2(a). Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure 2.2(b).
- Here the routing table of node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure 2.2(b)
- The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way.
- The end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination.
- Each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken-link information to the whole network.
- A node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination.
- Figure 2.3 shows the case when node 11 moves from its current position.

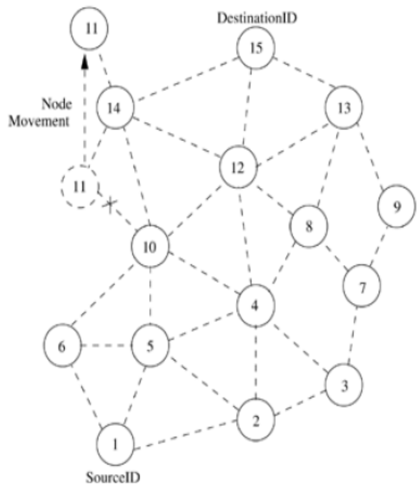


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

FIG .2.2 Route Establishment in Dsdv



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

FIG .2.3 Route Maintenance in Dsdv

Advantages

- Less delay involved in the route setup process.
- Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.
- The updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all nodes.

Disadvantages

- The updates due to broken links lead to a heavy control overhead during high mobility.
- Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.
- Suffers from excessive control overhead.
- In order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node.
- This delay could result in state routing information at nodes.

Wireless Routing Protocol (WRP)

- WRP is similar to DSDV; it inherits the properties of the distributed bellman-ford algorithm.
- To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and penultimate hop node on the path to every destination node.
- Maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.
- It differs from DSDV in table maintenance and in the update procedures.
- While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.

- The table that are maintained by a node are :

  - Distance table (DT): contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by the neighbor for a particular destination.

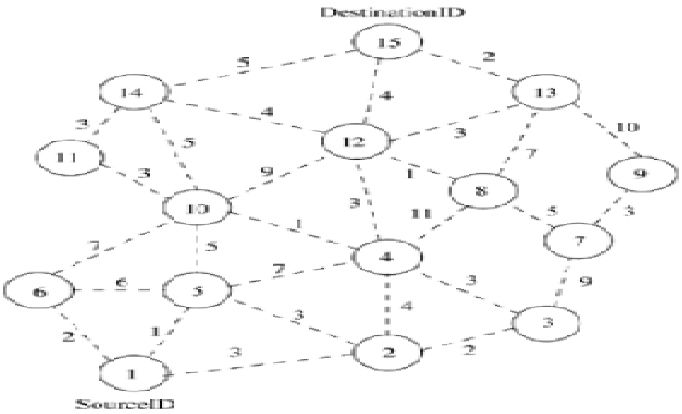
- Routing table (RT): contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor/penultimate node, the successor node, and a flag indicating the status of the path. The path status may be a simplest (correct) path or a loop (error), or destination node not marked (null).

- Link cost table (LCT): contains the cost of relaying messages through each link. The cost of broken link is ∞.it also contains the number of update periods passed since the last successful update was received from that link.

- Message retransmission list (MRL): contains an entry for every update message that is to be retransmitted and maintains a counter for each entry.

▪ After receiving the update message, a node not only updates the distance for transmitted neighbors but also checks the other neighbors' distance, hence convergence is much faster than DSDV.

▪ Consider the example shown in figure 2.4 below, where the source of the route is node 1 and destination is node 15. As WRP proactively maintains the route to all destinations, the route to any destination node is readily available at the source node.
▪ From the routing table shown, the route from node 1 to node 15 has the next node as node 2. The predecessor node of 15 corresponding to this route is route 12. The predecessor information helps WRP to converge quickly during link breaks.

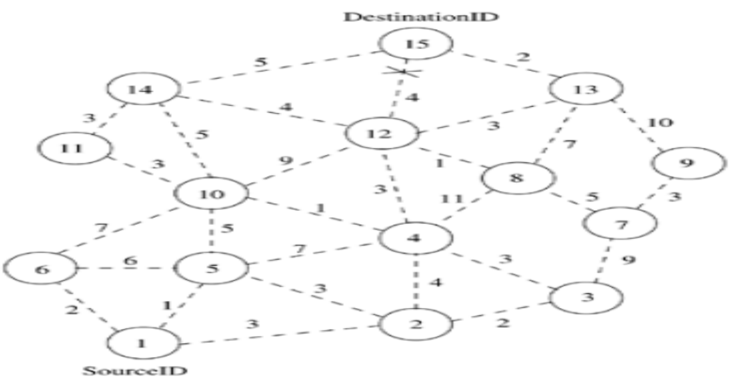


Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7
2	4	12	11
1	2	12	14

FIG .2.4 Route Establishment in WPS

▪ When a node detects a link break, it sends an update message to its neighbors with the link cost of the broken link set to ∞. After receiving the update message; all affected nodes update their minimum distances to the corresponding nodes. The node that initiated the update message then finds an alternative route, if available from its DT. Figure 2.5 shows route maintenance in WRP.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

FIG .2.5 Route maintenance in WPS

Advantages

- WRP has the same advantages as that of DSDV.
- It has faster convergence and involves fewer table updates.

Disadvantages

- The complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes in the adhoc wireless network.
- It is not suitable for highly dynamic and also for very large ad hoc wireless networks.

ON-DEMAND ROUTING PROTOCOLS

They execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination

Dynamic Source Routing Protocol (DSR)

- Designed to restrict the bandwidth consumed by control packets in adhoc wireless networks by eliminating the periodic table update messages
- It is beacon-less and does not require periodic hello packet transmissions
- Basic approach → to establish a route by flooding RouteRequest packets in the network
- Destination node responds by sending a RouteReply packet back to the source
- Each RouteRequest carries a sequence number generated by the source node and the path it has traversed
- A node checks the sequence number on the packet before forwarding it
- The packet is forwarded only if it is not a duplicate RouteRequest
- The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions
- Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase
- In figure 2.6, source node 1 initiates a RouteRequest packet to obtain a path for destination node 15
- This protocol uses a route cache that stores all possible information extracted from the source route contained in a data packet
- During network partitions, the affected nodes initiate RouteRequest packets
- DSR also allows piggy-backing of a data packet on the RouteRequest
- As a part of optimizations, if the intermediate nodes are also allowed to originate RouteReply packets, then a source node may receive multiple replies from intermediate nodes
- When an intermediate node in the path moves away, causing a wireless link to break, for example, the link between nodes 12 and 15 in Figure 2.7. Route Error message is generated from the node adjacent to the broken link to inform the source node. The source node reinitiates the route establishment procedure. The cached entries at the intermediate nodes and the source node are removed when a Route Error packet is received. If a link breaks due to the movement of edge nodes (nodes 1 and 15), the source node again initiates the route discovery process.

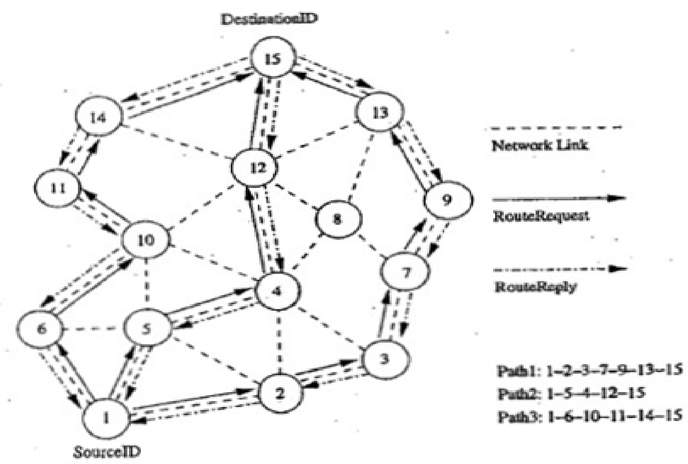


FIG .2.6 Route Establishment in DSR

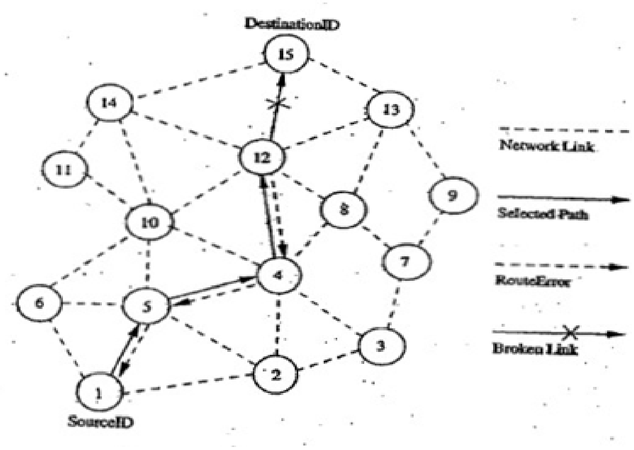


FIG .2.7 Route Maintenance in DSR

Advantages

- Uses a reactive approach which eliminates the need to periodically flood the network with table update messages
- Route is established only when required
- Reduce control overhead

Disadvantages

- Route maintenance mechanism does not locally repair a broken link
- Stale route cache information could result in inconsistencies during route construction phase
- Connection set up delay is higher
- Performance degrades rapidly with increasing mobility
- Routing overhead is more & directly proportional to path length

Ad Hoc On-Demand Distance Vector Routing Protocol

- Route is established only when it is required by a source node for transmitting data packets
- It employs destination sequence numbers to identify the most recent path
- Source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission
- Uses DestSeqNum to determine an up-to-date path to the destination
- A RouteRequest carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier and the time to live field
- DestSeqNum indicates the freshness of the route that is accepted by the source
- When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination
- The validity of the intermediate node is determined by comparing the sequence numbers
- If a RouteRequest is received multiple times, then duplicate copies are discarded
- Every intermediate node enters the previous node address and its BcastID
- A timer is used to delete this entry in case a RouteReply packet is not received.
- When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.
- AODV does not repair a broken path locally
- When a link breaks, the end nodes are notified
- Source node re-establishes the route to the destination if required

ROUTE ESTABLISHMENT IN AODV

- Consider the Figure 2.8. In this figure, source node 1 initiates a path-finding process by originating a RouteRequest to be flooded in the network for destination node 15, assuming that the RouteRequest contains the destination sequence number as 3 and the source sequence number as 1.
- When nodes 2, 5, and 6 receive the RouteRequest packet, they check their routes to the destination.
- In case a route to the destination is not available, they further forward it to their neighbors. Here nodes 3, 4, and 10 are the neighbors of nodes 2, 5, and 6. This is with the assumption that intermediate nodes 3 and 10 already have routes to the destination node, that is, node 15 through paths 10-14-15 and 3-7-9-13-15, respectively.
- If the destination sequence number at intermediate node 10 is 4 and is 1 at intermediate node 3, then only node 10 is allowed to reply along the cached route to the source. This is because node 3 has an older route to node 15 compared to the route available at the source node (the destination sequence number at node 3 is 1, but the destination sequence number is 3 at the source node), while node 10 has a more recent route (the Destination sequence number is 4) to the destination. If the RouteRequest reaches the destination (node 15) through path 4-12-15 or any other alternative route, the destination also sends a RouteReply to the source.
- In this case, multiple RouteReply packets reach the source. All the intermediate nodes receiving a RouteReply update their route tables with the latest destination sequence number. They also update the routing information if it leads to a shorter path between source and destination.

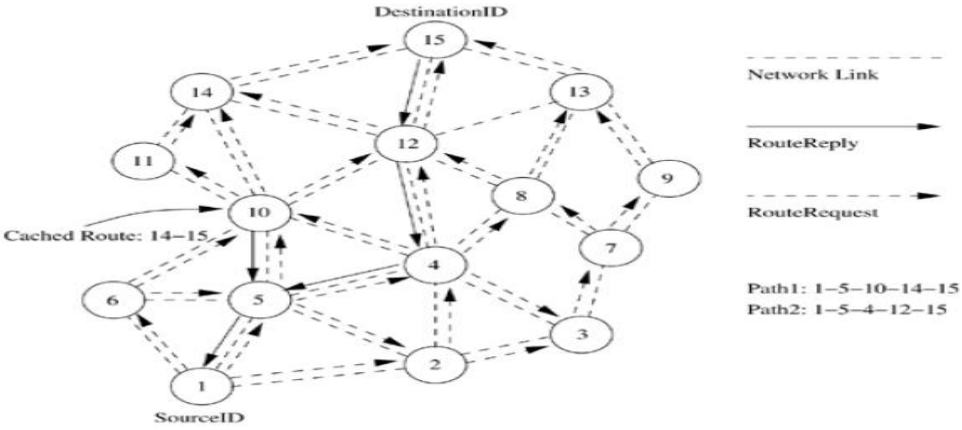


FIG 2.8.Route Establishment in AODV

Route maintenance in AODV

- AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or through link-level acknowledgments, the end nodes (i.e., source and destination nodes) are notified. When a source node learns about the path break, it reestablishes the route to the destination if required by the higher layers. If a path break is detected at an intermediate node, the node informs the end nodes by sending an unsolicited RouteReply with the hop count set as ∞.
- When a path breaks, for example, in fig 2.9 between nodes 4 and 5, both the nodes initiate RouteError messages to inform their end nodes about the link break. The end nodes delete the corresponding entries from their tables. The source node reinitiates the path finding process with the new BcastID and the previous destination sequence number.

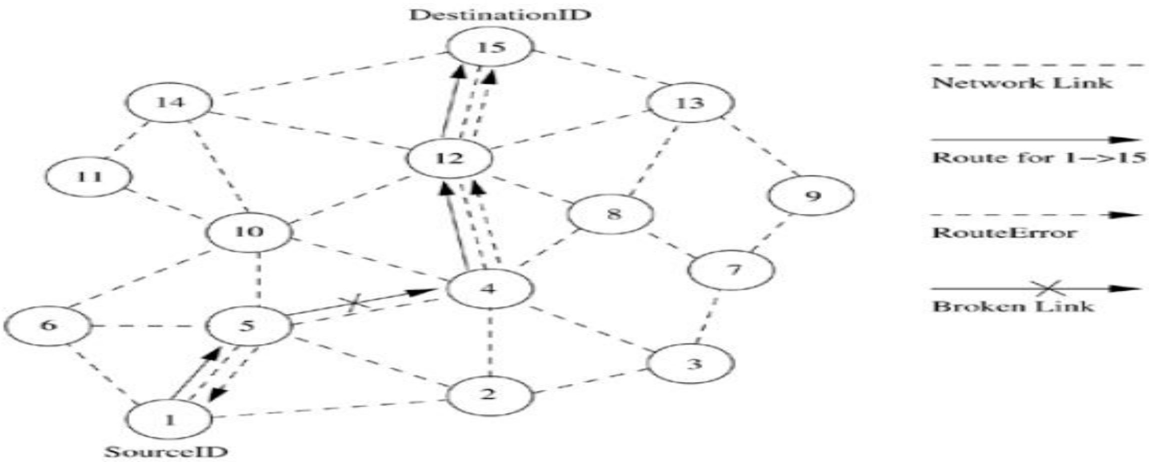


FIG 2.9.Route Maintenance in AODV

Advantage

- Routes are established on demand and DestSeqNum are used to find latest route to the destination
- Connection setup delay is less

Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old
- Multiple RouteReply packets to single RouteRequest packet can lead to heavy control overhead
- Periodic beaconing leads to unnecessary bandwidth consumption

HYBRID ROUTING PROTOCOLS

Here, each node maintains the network topology information up to m nodes.

Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR)

- CEDAR integrates routing and support for QoS.
- It is based on extracting core nodes (also called as Dominator nodes) in the network.
- Core nodes together approximate the minimum Dominating Set (DS).
- A DS of a graph is defined as a set of nodes such that every node in the graph is either present in the DS or is a neighbor of some node present in the DS.
- There exists at least one core node within every three hops.
- The nodes that choose a core node as their dominating node are called core member nodes of the core node concerned.
- The path between two core nodes is termed as virtual link.
- CEDAR employs a distributed Algorithm to select core nodes.
- The selection of core nodes represents the core extraction phase.
- CEDAR uses the core broadcast mechanism to transmit any packet throughout the network in the unicast mode, involving as minimum number of nodes as possible.
- Route Establishment in CEDAR: It is carried out in two phase.
- The first phase finds a core path from source to destination. The core path is defined as the path from dominator of the source node (source core) to the dominator of the destination node (destination core).
- In the second phase, a QoS feasible path is found over the core path.
- A node initiates a RouteRequest if the destination is not in the local topology table of its core node; otherwise the path is immediately established.
- For establishing a route, the source core initiates a core broadcast in which the RouteRequest is sent to all neighboring core nodes which in turn forwards it.
- A core node which has the destination node as its core member replies to the source core.
- Once the core path is established, a path with the requested QoS support is then chosen.

- A node after which the break occurred:
    - Sends a notification of failure.
    - Begins to find a new path from it to the destination.
    - Rejects every received packet till the moment it finds the new path to the destination.
- Meanwhile, as the source receives the notification message:
    - It stops to transmit.
    - Tries to find a new route to the destination.
    - If the new route is found by either of these two nodes, a new path from the source to the destination is established.
-

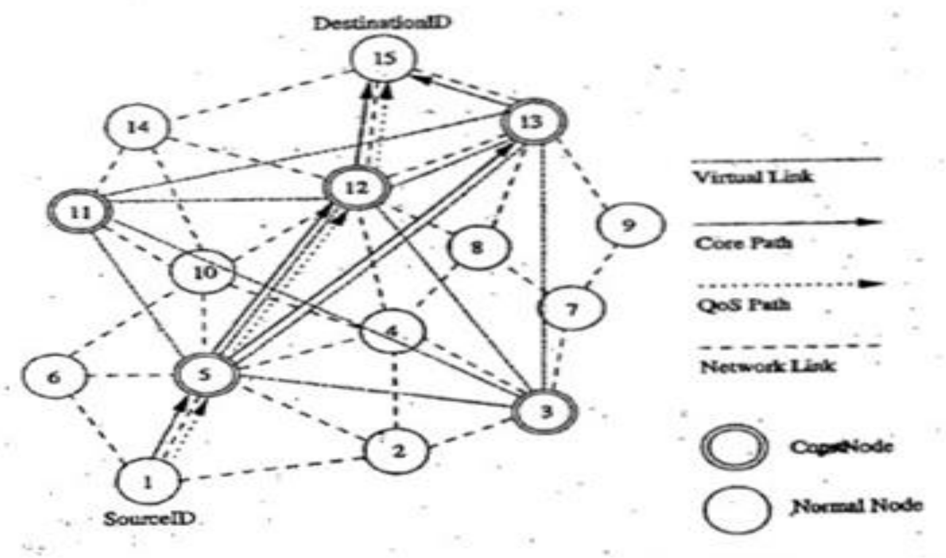


FIG 2.10.Route Establishment in CEDAR

Route Establishment in CEDAR

Consider Figure 2.10 where the source is node 1 and the destination is node 15. The core nodes in the network are nodes 3, 5, 11, 12, and 13. In this figure, node 5 is the dominator of nodes 1 and 6. Similarly, node 12 is the dominator of node 15. When node 1 initiates a RouteRequest to be flooded throughout the network, it intimates its core node the <source id, destination id> pair information. If the core node 5 does not have any information about the dominator of node 15, which is the destination node, it initiates a core broadcast. Due to this, all nearby core nodes receive the request in the unicast transmission mode. This unicast transmission is done on the virtual links. For core node 5, the virtual link with core node 3 comprises of the links 5-2 and 2-3, while the virtual link between core nodes 5 and 13 is represented by path 5-4-8-13. When a core node receives the core broadcast message, it checks whether the destination is its core member. A core node having the destination as one of its core members replies to the source core node. In our case, core node 12 replies to core node 5. The path between core nodes 12 and 5 constitutes a core path. Once a core path is established, the feasibility of the path in terms of the availability of the required Bandwidth is checked. If the required bandwidth is available on the path, the connection is established; otherwise, the core path is rejected.

Route Maintenance in CEDAR

CEDAR attempts to repair a broken route locally when a path break occurs. When a link u-v on the path from source to the destination fails, node u sends back a notification to the source and starts recomputation of a route from itself to the destination node. Until the route recomputation gets completed, node u drops every subsequent packet it receives. Once the source node receives the notification sent by node u, it immediately stops transmitting packets belonging to the corresponding flow, and starts computing a new route to the destination. If the link break occurs near the source, route recomputation at node u may take a long time, but the notification sent by node u reaches the source node very rapidly and prevents large packet losses. If the broken link is very close to the destination, the notification sent by node u might take a longer time to reach the source, but the route recomputation time at node u is small and hence large packet losses are again prevented. If the link break occurs somewhere near the middle of the path, then both the local route recomputation mechanism and the route break notification mechanism are not fast enough, and hence a considerable amount of packet loss occurs in this case.

Consider the network topology shown in Figure 2.11 when the link between nodes 12 and 15 breaks, node 12 tries to reconnect to the destination using an alternate path that satisfies the bandwidth requirement. It also notifies the source node about the link break. The source node tries to reconnect to the destination by reinitiating the route establishment process. In case node 12 does not have any other feasible path, then the alternate path 1-5-4-8-13-15 found by the source node is used for the further routing of packets

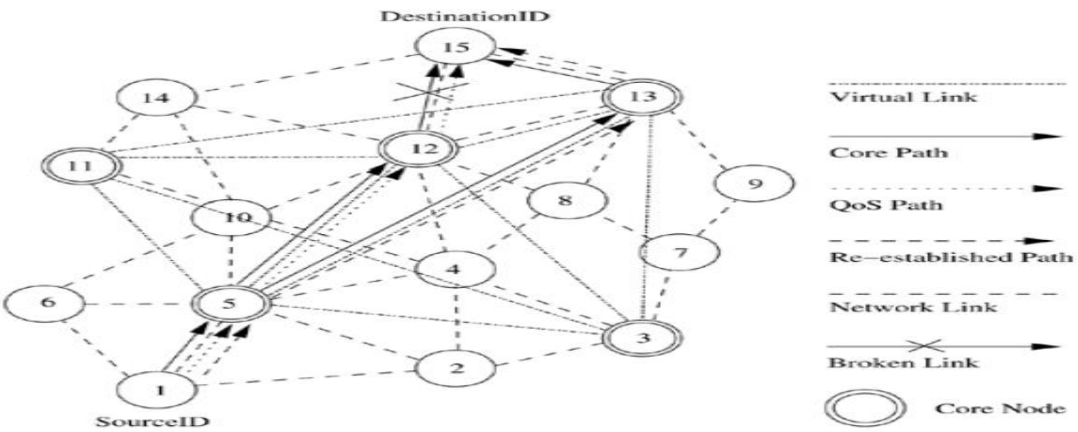


Fig 2.11Route Maintenance in CEDAR

Advantages

- Performs both routing and QoS path computation very efficiently with the help of core nodes.
- Utilization of core nodes reduces traffic overhead.

- Core broadcasts provide a reliable mechanism for establishing paths with QoS support.
-

Disadvantages

- Since route establishment is carried out at core nodes, the movement of core nodes adversely affects the performance of the protocol.
- Core node update information causes control overhead.

Zone Routing Protocol (ZRP)

- Effectively combines the best features of both Proactive and Reactive routing protocols.
- It use a Proactive routing scheme within a limited zone in the r-hop neighborhood of every node.
- Use a Reactive routing scheme for nodes beyond this.
- An Intra-Zone Routing Protocol (IARP) is used in the zone where a particular node employs proactive routing.
- The Reactive routing protocol used beyond this zone is referred to as Inter-Zone Routing Protocol (IERP).

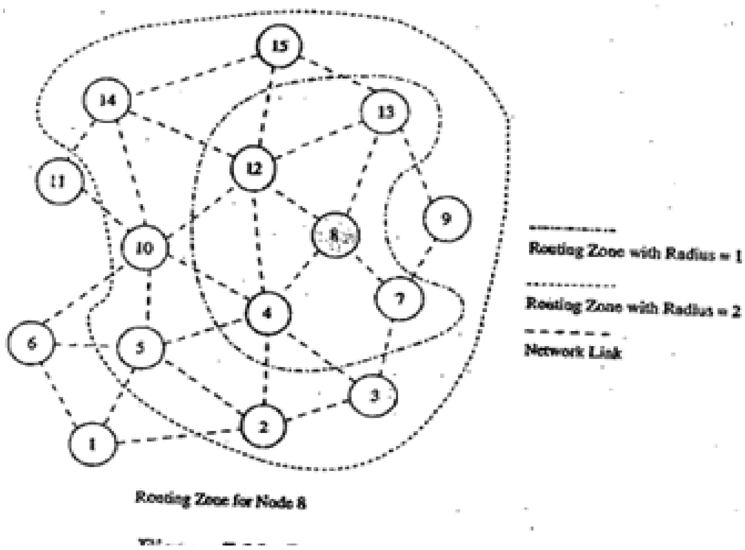


Fig 2.12 Route Establishment

- The routing zone of a given node is a subset of the network, within which all nodes are reachable within less than or equal to.
- Route Establishment: When a node s (node 8 in the fig 2.12) has packets to be sent to a destination node d (node 15 in fig), it checks whether node d is within its zone.
- If the destination belongs to its own zone, then it delivers the packets directly.
- Otherwise, node s broadcasts the RouteRequest to its peripheral nodes (in fig, node 8 broadcasts RouteRequest to node 2, 3, 5, 7, 9, 10, 13, 14 and 15).
- If any peripheral node finds node d to be located within its routing zone, it sends a RouteReply back to node 8 indicating the path; otherwise, the node rebordercasts the RouteRequest packet to the peripheral nodes.
- This process continues until node d is located.
- During RouteRequest propagation, every node that forwards the RouteRequest appends its address to it.
- This information is used for delivering the RouteReply packet back to the source.
- The criteria for selecting the best path may be the shortest path, least delay path etc.
- When an intermediate node in an active path detects a broken link in the path, it performs a local path reconfiguration in which the broken link is bypassed by means of a short alternate path connecting the ends of the broken link

- A path update message is then sent to the sender node
- This results in sub-optimal path between two end points.

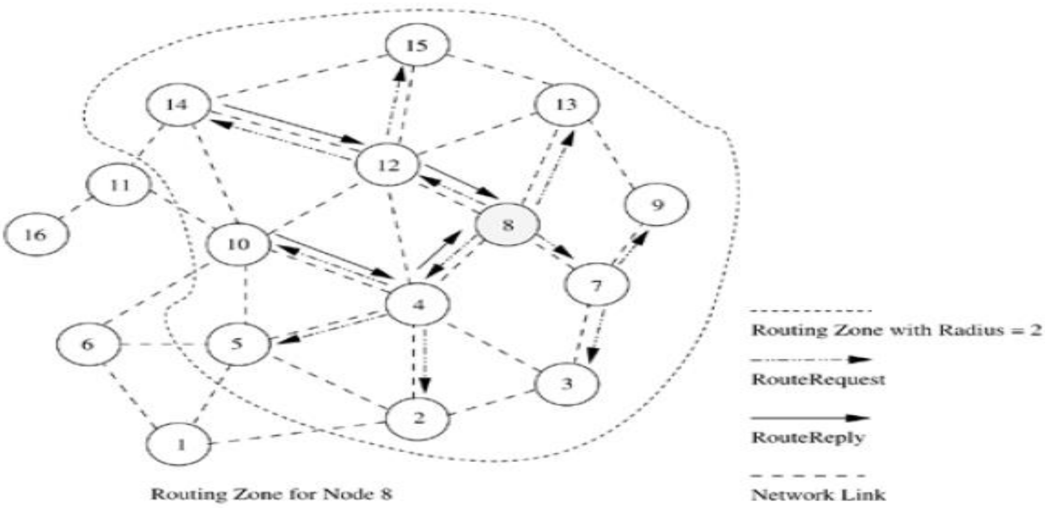


Fig 2.13. Path finding between node 8 and node 16.

Advantage
Reduce the control overhead by combining the best features of Proactive and Reactive protocols.

Disadvantage
Control overhead may increase due to the large overlapping of nodes routing zones.