UNIT 5

Routing Protocols

Introduction

A variety of routing protocols for ad hoc wireless networks has been proposed in the recent past. This chapter first presents the issues involved in designing a routing protocol and then the different classifications of routing protocols for ad hoc wireless networks. It then discusses the working of several existing routing protocols with illustrations.

4.1 Issues in designing a routing protocol

The major challenges that a routing protocol designed for ad hoc wireless networks faces are mobility of nodes, resource constraints, error-prone channel state, and hidden and exposedterminal problems. A detailed discussion on each of the following is given below.

4.1.1 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.

4.1.2 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 routing protocols inmaintaining the topological information.

4.1.3 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.

4.1.4 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 4.1. 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.

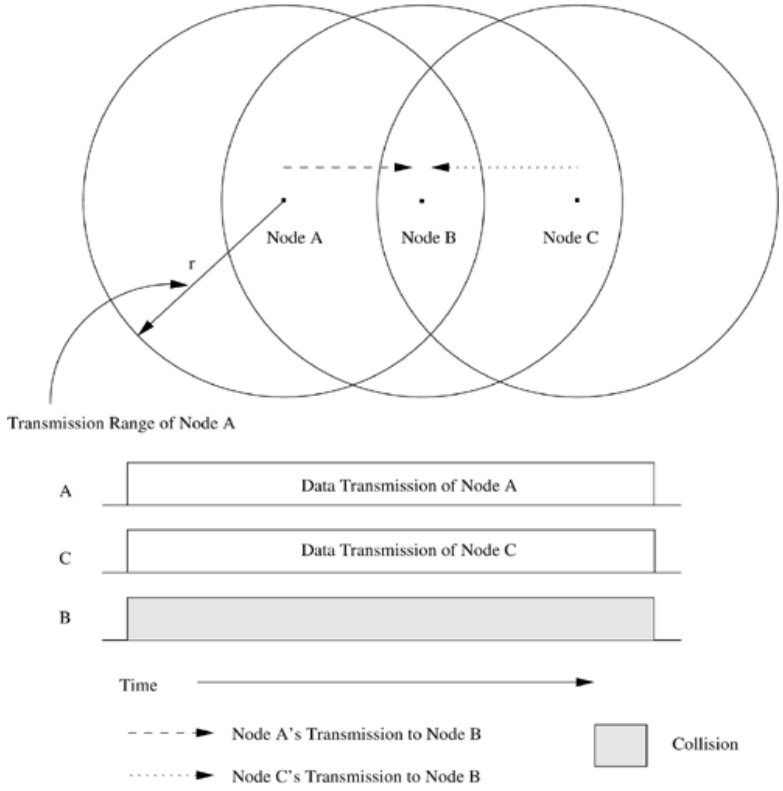


Figure 4.1. Hidden terminal problem.

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. Consider the example in Figure 4.3. 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. For node C to transmit simultaneously when node B is transmitting, the transmitting frequency of node C must be different from its receiving frequency.

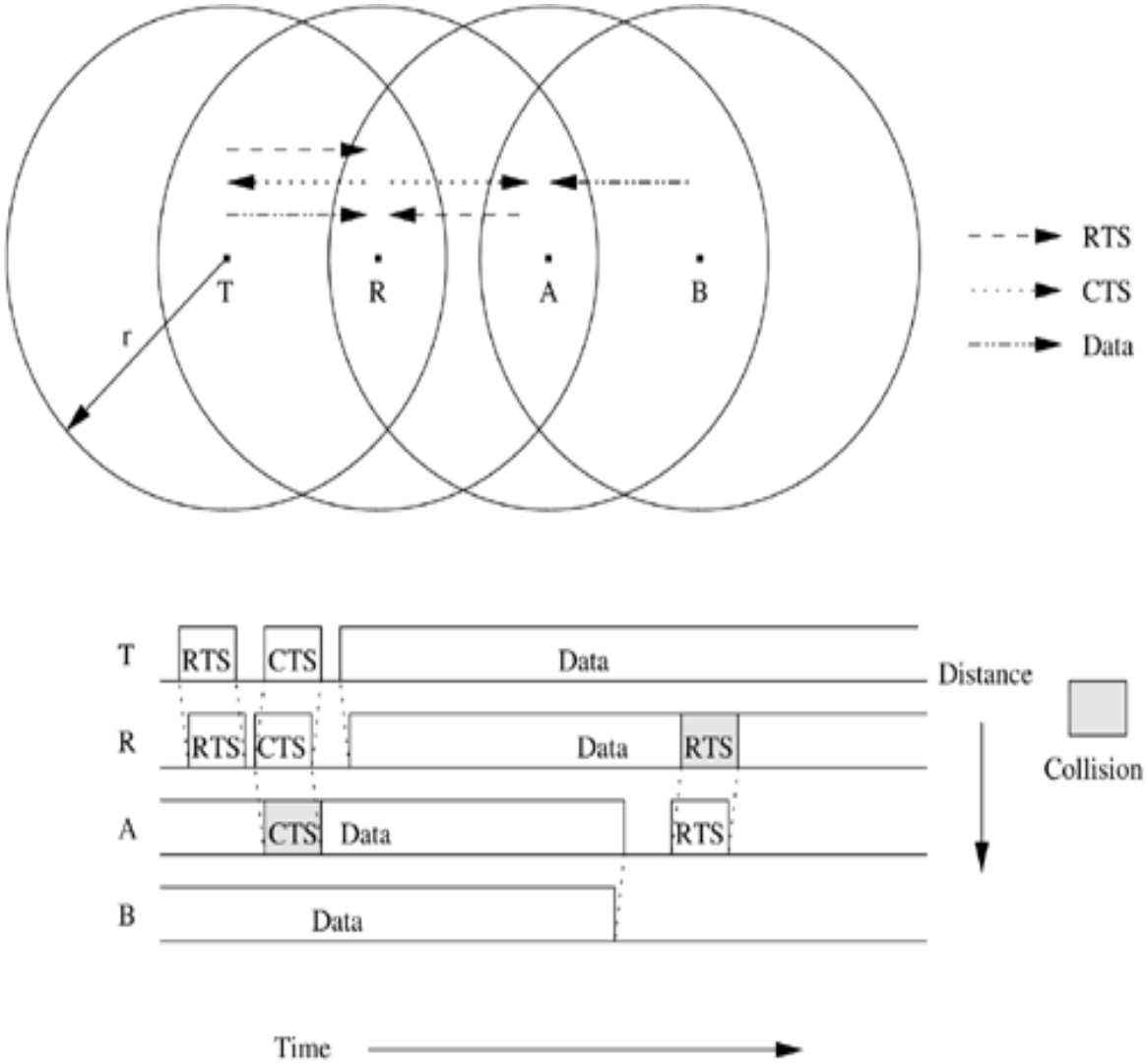


Figure 4.2. Hidden terminal problem with RTS-CTS-Data-ACK scheme.

Solution for this problem includes 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.

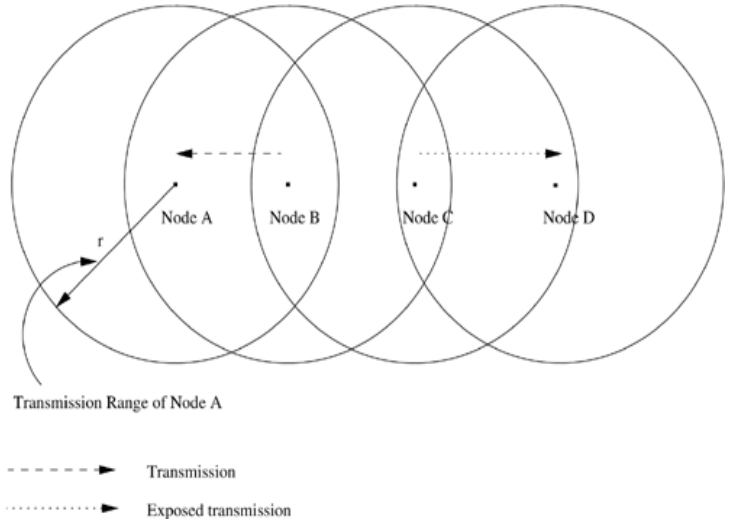


Figure 4.3. Exposed terminal problem**.**

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 4.3. 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.

4.2 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.

4.3 Classifications of Routing Protocols

The routing protocols for ad hoc wireless networks can be broadly classified into four categories based on

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

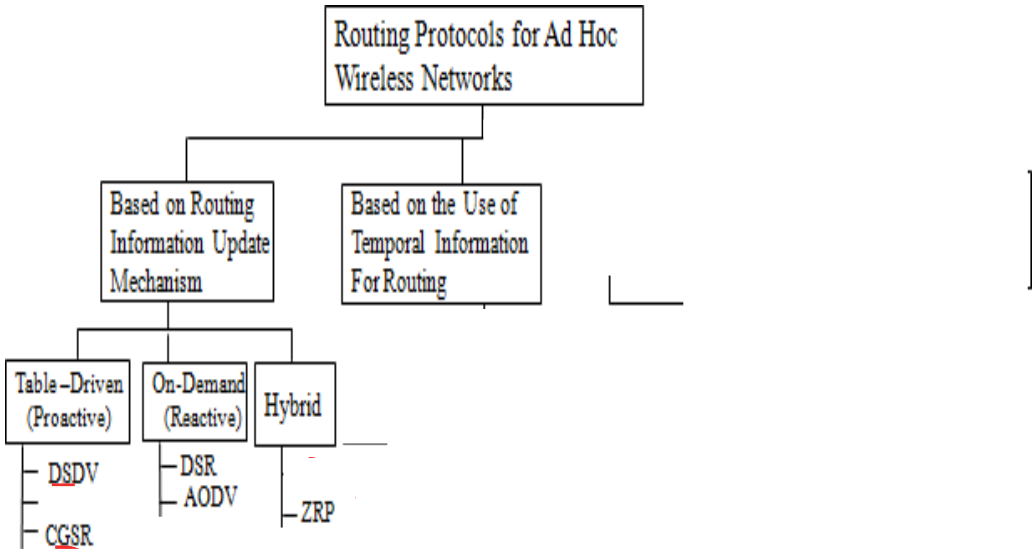


Figure 4.4. Classifications of routing protocols.

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.

4.3.1 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

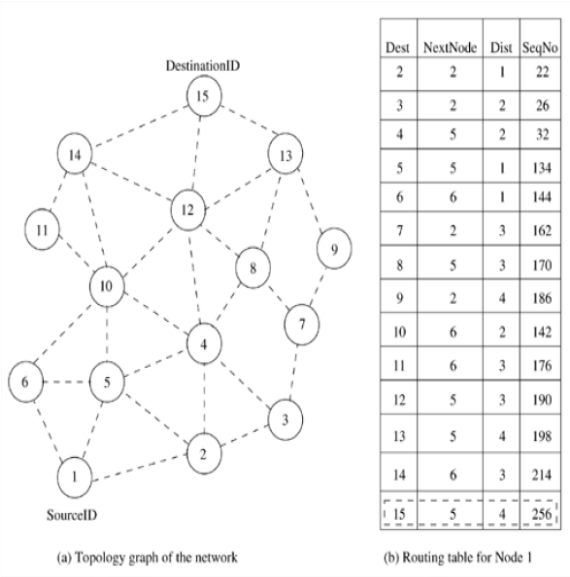
Ex: Destination sequenced distance vector routing protocol (DSDV), wireless routing protocol (WRP), source-tree adaptive routing protocol (STAR) and cluster-head gateway switch routing protocol (CGSR).

4.3.1.1 Destination sequenced distance-vector routing protocol

- 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 4.5 (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 4.5 (b).
- Here the routing table 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 (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 it neighbors in order to propagate the broken-link information to the whole network.
- A node always assigns an odd number to the link break update to differentiate it from the even sequence number generated by the destination.
- Figure 4.6 shows the case when node 11 moves from its current position.

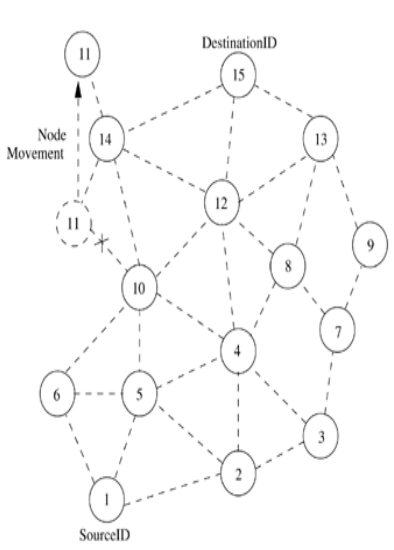


(a) Topology graph of the network

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

Figure 4.5. 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

Figure 4.6. 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.

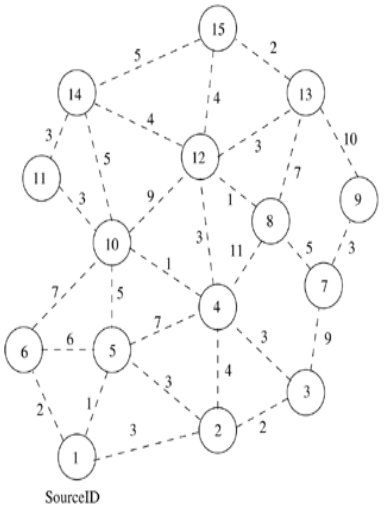
Disadvantages

- 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.

4.3.1.2 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. Itcontains a matrix where each element contains the distance and the penultimate nodereported 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.

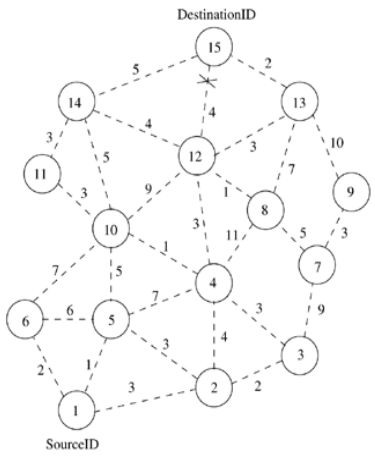
- Consider the example shown in figure below, where the source of the route is node 1 and destination is node 15. As WRP proactively maintains the route to all destinations, the route to any destination node is readily available at the source node.
- From the routing table shown, the route from node 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

Figure 4.7. Route establishment 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

Figure 4.8. Route maintenance in WRP.

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 4.8 shows route maintenance in WRP.

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.

4.3.1.3 Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Uses a hierarchical network topology, CGSR organizes nodes into clusters, with coordination among the members of each cluster entrusted to a special node named *cluster-head.* This cluster-head is elected dynamically by employing a least cluster change (LCC) algorithm.

- According to this algorithm, a node ceases to be a cluster-head only if it comes under the range of another cluster-head, where the tie is broken either using the lowest ID or highest connectivity algorithm.
- Clustering provides a mechanism to allocate bandwidth, which is a limited resource, among different clusters, thereby improving reuse.
- A token-based scheduling is used within a cluster for sharing the bandwidth among the members of the cluster.
- CGRS assumes that all communication passes through the cluster-head. Communication between 2 clusters takes place through the common member nodes that are members of both the cluster are called *gateways.*
- A gateway is expected to be able to listen to multiple spreading codes that are currently in operation in the clusters in which the node exists as a member.
- A gateway conflict is said to occur when a cluster-head issues a token to a gateway over spreading code while the gateway is tuned to another code.
- Gateways that are capable of simultaneously communicating over two interfaces can avoid gateway conflicts.
- The performance of routing is influenced by token scheduling and code scheduling that is handled at cluster-heads and gateways, respectively.
- Every member node maintains a routing table containing the destination cluster-head for every node in the network.
- In addition to the cluster member table, each node maintains a routing table which keeps the list of next-hop nodes for reaching every destination cluster.
- The cluster routing protocol is used here.
- Figure below shows the cluster head, cluster gateways, and normal cluster member nodes in an ad hoc wireless network.

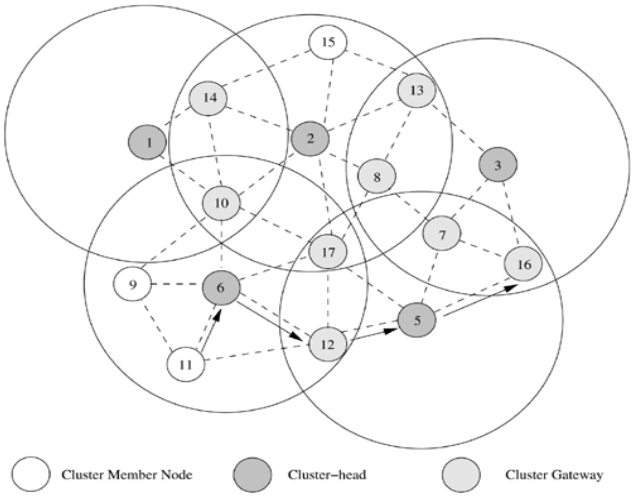


Figure 4.9. Route establishment in CGSR**.**

Advantages

- CGSR is a hierarchical routing scheme which enables partial coordination between nodesby electing cluster-heads.
- Better bandwidth utilization is possible.
- Easy to implement priority scheduling schemes with token scheduling and gateway codescheduling.

Disadvantages

- Increase in path length and instability in the system at high mobility when the rate ofchange of cluster-head is high.
- In order to avoid gateway conflicts, more resources are required.
- The power consumption at the cluster-head node is also a matter of concern.
- Lead to Frequent changes in the cluster-head, which may result in multiple path breaks.

4.3.2 On-Demand Routing Protocols

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

4.3.2.1 Dynamic Source Routing Protocol (DSR)

- Designed to restrict the bandwidth consumed by control packets in adhoc wirelessnetworks by eliminating the periodic table update messages.
- It is beacon-less and does not require periodic hello packet transmissions.
- Basic approach is to establish a route by flooding Route Request packets in the network.
- Destination node responds by sending a Route Reply packet back to the source.
- Each Route Request carries a sequence number generated by the source node and the pathit 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 Route Request.
- 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 Route Request packet during the route construction phase. In figure 4.10, source node 1 initiates a Route Request 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 Route Request packets.
- DSR also allows piggy-backing of a data packet on the Route Request.
- As a part of optimizations, if the intermediate nodes are also allowed to originate Route

Reply packets, then a source node may receive multiple replies from intermediate nodes.

- In fig 4.11, if the intermediate node 10 has a route to the destination via node 14, it also sends the Route Reply to the source node.
- The source node selects the latest and best route and uses that for sending data packets.
- Each data packet carries the complete path to its destination.
- If a link breaks, source node again initiates the route discovery process

All the intermediate nodes flood the *Route Request* packet if it is not redundant. For example, after receiving the *Route Request* packet from node 1 (refer to Figure 4.10), all its neighboring nodes, that is, nodes 2, 5, and 6, forward it. Node 4 receives the *Route Request* from both nodes 2 and 5. Node 4 forwards the first *Route Request* it receives from any one of the nodes 2 and 5 and discards the other redundant/duplicate *Route Request* packets. The *Route Request* is propagated till it reaches the destination which initiates the *Route Reply*. As part of optimizations, if the intermediate nodes are also allowed to originate *Route Reply* packets, then a source node may receive multiple replies from intermediate nodes. For example, in Figure 4.11, if the intermediatenode 10 has a route to the destination via node 14, it also sends the *Route Reply* to the source

node. The source node selects the latest and best route, and uses that for sending data packets. Each data packet carries the complete path to its destination. A *RouteError* 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*RouteError* 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.

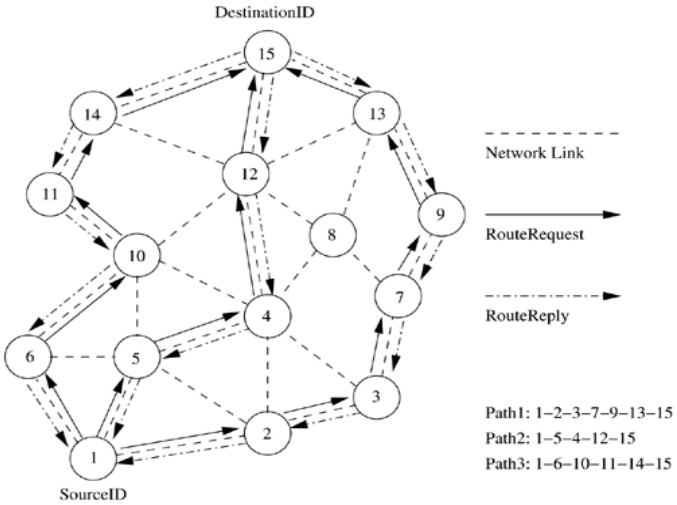


Figure 4.10. Route establishment in DSR.

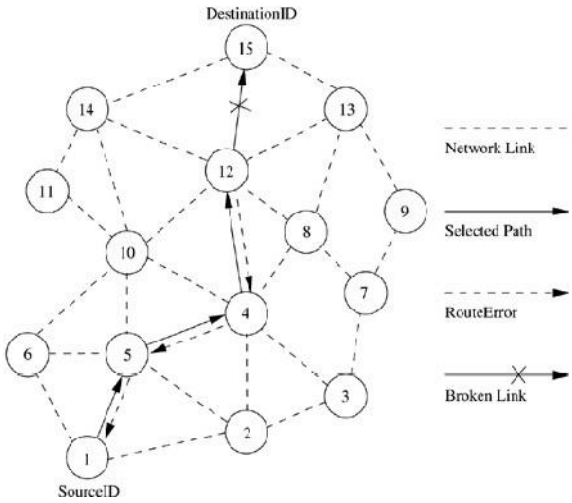


Figure 4.11. Route maintenance in DSR.

Advantages

- Uses a reactive approach which eliminates the need to periodically flood the networkwith 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 constructionphase.
- Connection set up delay is higher.
- Performance degrades rapidly with increasing mobility.
- Routing overhead is more & directly proportional to path length

4.3.2.2 Ad Hoc On-Demand Distance Vector Routing Protocol (AoDV)

- Route is established only when it is required by a source node for transmitting datapackets.
- It employs destination sequence numbers to identify the most recent path.
- Source node and intermediate nodes store the next hop information corresponding to eachflow 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 isused to delete this entry in case a RouteReply packet is not received. 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.

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 arethe 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 thesource 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.

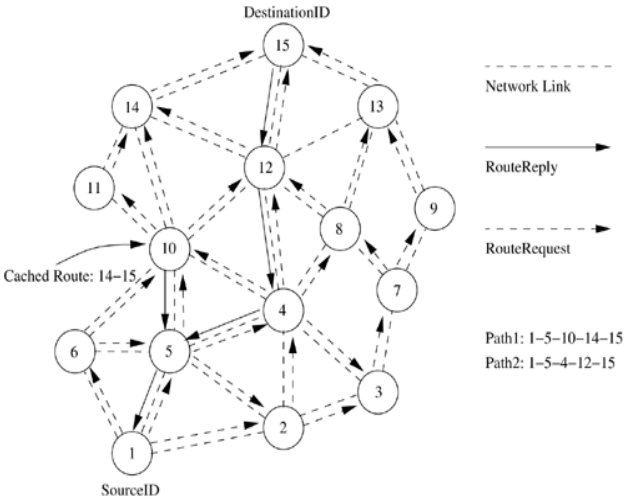


Figure 4.12. Route establishment in AODV.

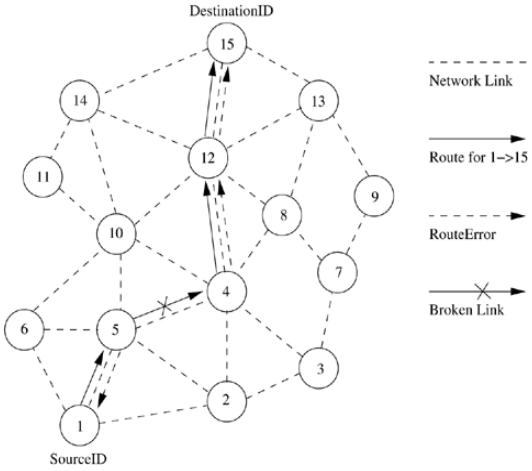


Figure 4.13. Route maintenance in AODV.

Advantages

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

Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is veryold.
- Multiple RouteReply packets to single RouteRequest packet can lead to heavy controloverhead.
- Periodic beaconing leads to unnecessary bandwidth consumption

4.4 Hybrid Routing Protocols

Here, each node maintains the network topology information up to *m* hops. The different existinghybrid protocols are presented below.

4.4.1 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 eitherpresent 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 membernodes of the core node concerned.
- The path between two core nodes is termed as virtual link. CEDAR employs a distributedAlgorithm 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 thenetwork 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 asthe 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 itscore node; otherwise the path is immediately established.
- For establishing a route, the source core initiates a core broadcast in which theRouteRequest is sent to all neighboring core nodes which inturn 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 tothe destination is established.

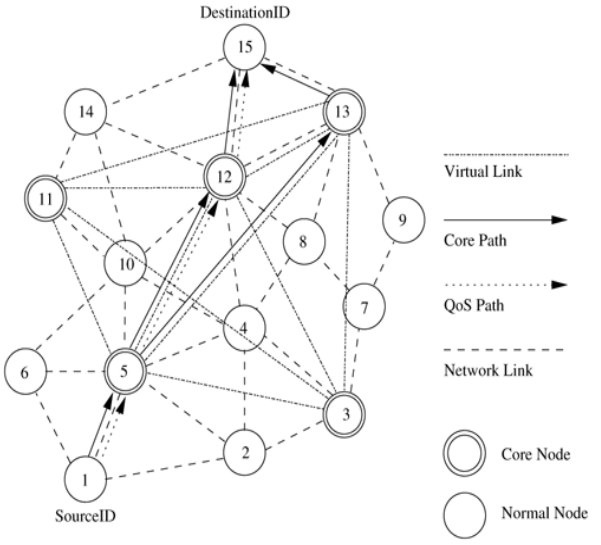


Figure 4.20 Route establishment in CEDAR.

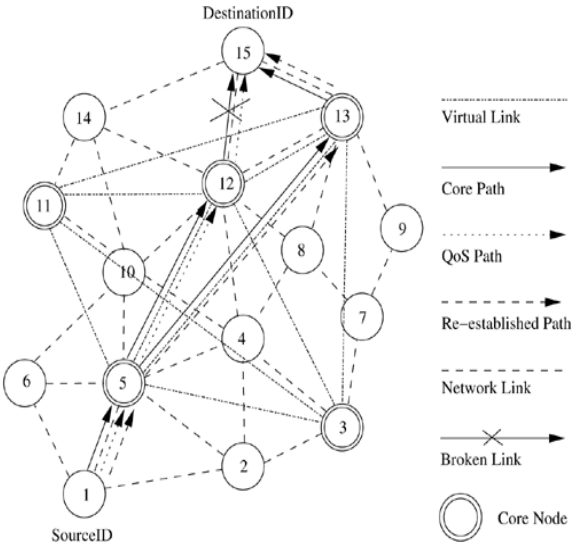


Figure 4.21 Route maintenance in CEDAR.

Advantages

- Performs both routing and QoS path computation very efficiently with the help of corenodes.
- 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 nodesadversely affects the performance of the protocol.
- Core node update information causes control overhead.

4.4.2 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 ofevery 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 RoutingProtocol (IERP).

- The routing zone of a given node is a subset of the network, within which all nodes arereachable within less than or equal to.

Route Establishment: When a node s (node 8 in the fig 4.22) has packets to be sent to adestination 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 performsa 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.

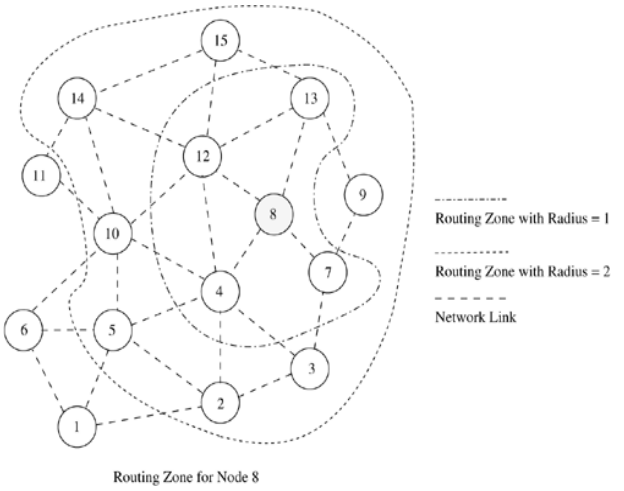


Figure 4.22. Routing zone for node 8 in ZRP.

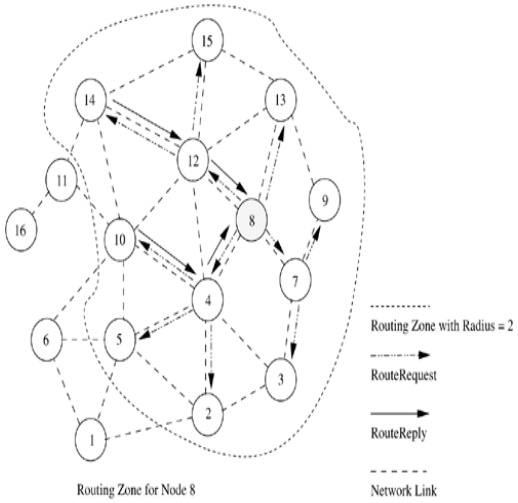


Figure 4.23. Path finding between node 8 andnode 16.

Advantage

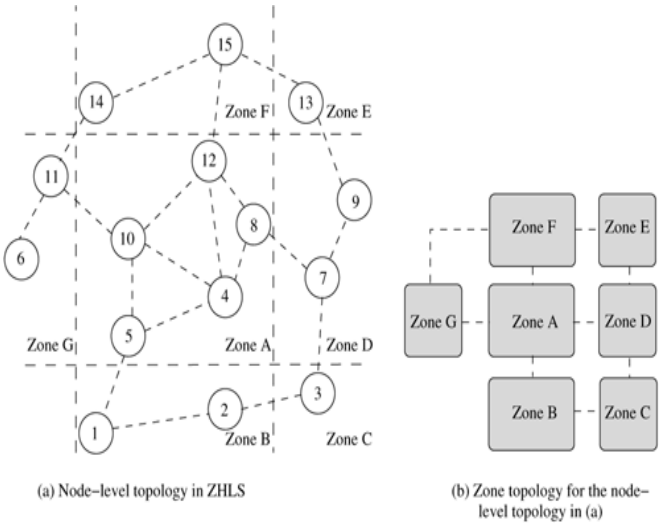
- Reduce the control overhead by combining the best features of Proactive and Reactiveprotocols.

Disadvantage

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

4.4.3 Zone Based Hierarchical Link State Routing Protocol (ZHLS)

- ZHLS uses the geographical location info of the nodes to form non-overlapping zones. AHierarchical Addressing that consists of a zone ID and a node ID is employed.
- Similar to ZRP, ZHLS also employs a Proactive approach inside the geographical zoneand a Reactive approach behind the zone.
- Every node requires GPS support for obtaining its own geographical location that is usedto map itself into corresponding zone.
- The assignment of zone addresses to geographical areas is important and is done during aphase called the network design phase or network deployment phase.
  i. Each node maintains two link state packets: (LSP)
  ii. Node level LSP: list of connected neighbors.
  iii. Zone LSP: list of connected zones.
- Route Establishment, If a source node src wants to communicate with a destination node dest, src checks whether dest resides in its own zone.
- If dest belongs to same zone, then packets are delivered to the dest as per the Intra-Zone routing table.
- If dest does not belong to the same zone, then the src originates a location request packet containing the sender's and destination's information. This location info is forwarded to every other zone.
- The gateway node of a zone at which the location request packet is received verifies its routing table for the destination node.
- The gateway node that finds the destination node required by a location request packet originates a location response packet containing the zone information to the sender.



(a) Node–level topology in ZHLS

(b) Zone topology for the node–level topology in (a)

Table 4.1. Zone link state packets

Source Zone	Zone Link State Packet
A	B, D, F, and G
B	C and A
C	B and D
D	A, C, and E
E	A, D, and F
F	A, E, and G
G	A and F

Figure 4.24. Zone-based hierarchical link state routing protocol.

Route Maintenance

- If a given gateway node away causing a zone level connection failure, routing can

stilltake place with the help of the other gateway nodes.

- This is due to the hierarchical addressing that makes use of zone ID and node ID.

4.5 Routing Protocols With Efficient Flooding Mechanisms

- Many protocols flood the network with RouteRequest packets in order to obtain a path to the destination.
- Flooding of control packets results in:
  - Wastage of bandwidth.
  - Increase in number of collisions.
- Protocols with efficient flooding mechanisms:
  - Preferred link-based routing (PLBR) protocol.
  - Optimized link state routing (OLSR) protocol.

Preferred Link Based Routing (PLBR) Protocols

- Use the preferred link approach in an implicit manner by processing a RouteRequest packet only if it is received through a strong link.
- Here a node selects a subset of nodes from its Neighbors List (NL). This subset is referred to as the Preferred List (PL) selection of this subset may be based on link or nodecharacteristics.
- All neighbors receive RouteRequest packets because of the broadcast radio channel, but only neighbors present in the PL forward them further.
- Each node maintains information about its neighbors and their neighbors in a table called Neighbor's Neighbor Table (NNT). It periodically transmits a beacon containing the changed neighbor's information.

Route Establishment

- If dest is in src's NNT, the route is established directly. Otherwise, src transmits a RouteRequest packet containing
  - Source node's address (SrcID)
  - Destination node's address (DestID)
  - Unique sequence number (SeqNum)
  - Traversed path (TP)
  - PL
  - TTL flag
  - NoDelay flag
- A node is eligible for forwarding a RouteRequest only if it satisfies the following criteria:
- The node ID must be present in the received RouteRequest packet's PL.

- RouteRequest packet must not have been already forwarded by the node, and the TTL onthe packet must be greater than zero.
- If the dest is in the eligible node's NNT, the RouteRequest is forwarded as a unicast packet to the neighbor.
- If the computed PLT is empty, the RouteRequest packet is discarded and marked as sent.
- If the RouteRequest reaches the destination, the route is selected by the route selection procedure given below.

Route selection

- When multiple Route Request packets reach dest,the route selection procedure selects thebest route among them.
- The criterion for selecting the best route can be the shortest path, or the least delay path, or the most stable path.
- Dest starts a timer after receiving the first route request packet. The timer expires after a certain RouteSelectWait period, after which no more RouteRequest packets would be accepted.
- From the received Route Request packets, a route is selected as follows:
- For every RouteRequest i that reached Dest during the RouteSelectWait period, Max(Wmin) is selected, where is the min. Weight of the link in the path followed by i if two or more paths have the same value for the shortest path is selected.
- After selecting a route, all subsequent RouteRequest packets from the same src with a seqnum less than or equal to the seqnum of the selected RouteRequest are discarded.
- If the node delay flag is set, the route selection procedure is omitted and TP of the first RouteRequest reaching the Dest is selected as the route.

Algorithms for preferred links computation:

Neighbor-Degree-Based preferred link algorithm (NDPL) Weight Based preferred link algorithm(WBPL)

NDPL (Neighbor-Degree-Based preferred link algorithm)

Let d → node that calculates the preferred list table PLT. TP Traversed path. OLDPL → preferred list of the received RouteRequest packet. NNTd → NNT of the node d. N(i) → neighbors of node I and itself. INL→ include list, a set containing all reachable neighbors by transmitting the RouteRequest packet. EXL → Exclude list, a set containing all neighbors that are unreachable by transmitting the RouteRequest packet after execution of the algorithm.

Step 1: Node d marks the nodes that are not eligible for further forwarding the RouteRequest packet.

a) If a node i of TP is a neighbor of node d mark all neighbors of i as reachable i.e add N(i)to INL.

b) If a node i of OLDPL is a neighbor of node d and i < d, then include N(i) in INL.

c) If neighbor i of node d has a neighbor n present in TP, add N(i) to INL.

d) If neighbor i of node d has a neighbor n present in OLDPL and n < d, add N(i) to INL.

Step 2: If neighbor i of node d is not in INL, put i in PLT and mark all neighbor of i as reachable. If i is present in INL, mark the neighbors of i as unreachable by adding them to EXL. **Step 3:** If neighbor i of d has a neighbor n present in EXL, put i in PLT and mark all neighborsof i as reachable. Delete all neighbors of i from EXL.

Step 4: Reduction steps are applied here in order to remove overlapping neighbors from PLT without compromising on reachability.

a) Remove each neighbor i from PLT if N (i) is covered by remaining neighbors of PLT. Here the minimum degree neighbor is selected every time.

b) Remove neighbor i from PLT whose N (i) is covered by node d itself.

Weight-Based Preferred Link Algorithm (WBPL)

In this algorithm, a node finds the preferred links based on stability, which is indicated by a weight, which in turn is based on its neighbors' temporal and spatial stability.

1. Let $BCnt_i$ be the count of *beacons* received from a neighbor i and TH_{bcon} is the number of beacons generated during a time period equal to that required to cover twice the transmission range $(TH_{bcon} = \frac{2 \times transmission\ range}{maximum\ velocity \times period\ of\ beacon})$. Weight given to i based on time stability (WT^i_{time}) is

$$WT_{time} = \begin{cases} 1 & \text{if } BCnt_i > TH_{bcon} \\ BCnt_i/TH_{bcon} & \text{otherwise.} \end{cases}$$

2. Estimate the distance (D^i_{Est}) to i from the received power of the last few packets using appropriate propagation models. The weight based on spatial stability is $WT^i_{spatial} = \frac{R - D_{Est}}{R}$.
3. The weight assigned to the link i is the combined weight given to time stability and spatial stability. $W_i = WT^i_{time} + WT^i_{spatial}$.
4. Arrange the neighbors in a non-increasing order of their weights. The nodes are put into the *PLT* in this order.
5. If a link is overloaded, delete the associated neighbor from *PLT*. Execute *Step* 1 of NDPL and delete $\forall i, i \in PLT \cap i \in INL$. Also, delete those neighbors from *PLT* that satisfy *Step* 4 of NDPL.

Advantages

- Minimizes broadcast storm problem. Hence, highly scalable.
- Reduction in control overhead results in decrease in the number of collisions andimprovement in efficiency of the protocol.

Disadvantage

- Computationally more complex.

4.5.1 Optimized Link State Routing (OLSR)

- It is a proactive routing protocol that employs an efficient link state packet forwardingmechanism called multipoint relaying (MPR).
- This protocol optimizes the pure link state routing protocol.
- Optimizations are done in two ways:
  - By reducing the size of control packets.
  - By reducing the no. of links that are used for forwarding the link state packets.
- The subset of links or neighbors that are designated for link state updates and areassigned the responsibility of packet forwarding are called multipoint relays.
- The set consisting of nodes that are multipoint relays is referred to as MPRset.
- Each node(say, P) in the n/w selects an MPRset that processes and forwards every linkstate packet that node P originates.
- The neighbor nodes that do not belong to the MPRset process the link state packetsoriginated by node P but do not forward them.
- Similarly, each node maintains a subset of neighbors called MPR selectors, which isnothing but the set of neighbors that have selected the node as a multipoint relay.
- In order to decide on the membership of the nodes in the MPRset, a node periodicallysends *Hello* messages that contain:
  - List of neighbors with which the node has bidirectional links
  - List of neighbors whose transmission was received in the recent past but with whombidirectional links have not yet been confirmed.
- The nodes that receive this Hello packet update their own two-hop topology tables.
- The selection of multipoint relays is also indicated in the Hello packet.
- The Data structure called neighbor table is used to store the list of neighbors, the two-hopneighbors, and the status of neighbor nodes.
- The neighbor nodes can be in one of the three possible link status states, i.e
  - Unidirectional

    Bidirectional

Multipoint relay

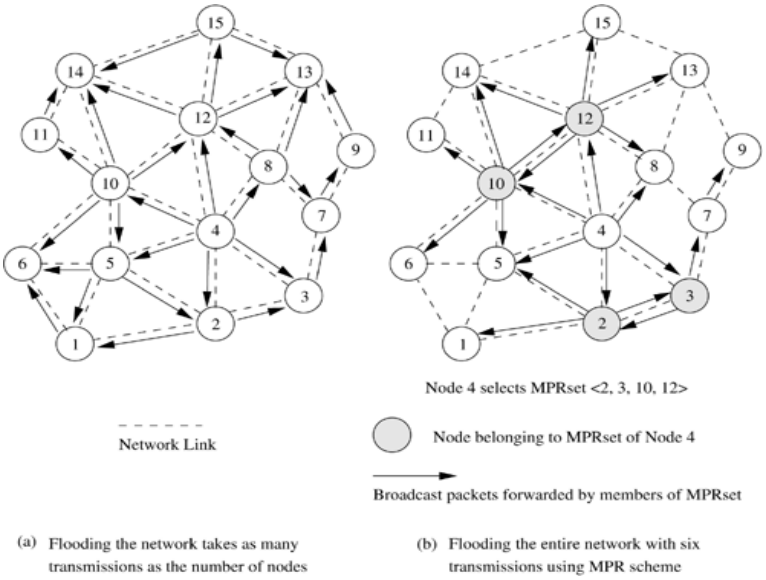


Figure 4.25. An example selection of MPRset in OLSR.

Selection of multipoint relay nodes (refer fig b) Ni(x) → ith hop neighbor set of node x MPR(x) → MPRset of node x.

Step1: MPR(x) ← Ø /* initializing empty MPRset */

Step2: MPR(x) ← {those nodes that belong to N1(x) and which are the only neighbors of nodesin N2(x)}

Step3: while there exists some node in N2(x) which is not covered by MPR(x)

a) For each node in N1(x),which is not in MPR(x),compute the maximum number of nodesthat it covers among the uncovered nodes in the set N2(x).

b) Add to MPR(x) the node belonging to N1(x) for which this number is maximum.

Advantages:

- Reduces the routing overhead.
- Reduces the no. of broadcasts done.
- Hence low connection setup time and reduced control overhead.

4.6 Hierarchical Routing Protocols

The use of routing hierarchy has several advantages Reduction in size of routing tables andbetter scalability.

4.6.1 Hierarchical State Routing (HSR) protocol

- It is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering.
- Each cluster has its leader.
- Clustering is organized in levels:

- **Physical**: between nodes that have physical wireless one-hop links between them.
- **Logical**: based on certain relations.

- Figure 4.26 illustrates the multilayer clustering defined by the HSR protocol. At the lowest level *(L* = 0), there are six cluster leaders (nodes 1, 2, 3, 4, 5, and 6). Nodes areclassified as cluster leaders, or gateway nodes, or normal member nodes.
- A cluster leader is entrusted with responsibilities such as slot/frequency/code allocation, call admission control, scheduling of packet transmissions, exchange of routing information, and handling route breaks. In Figure 4.27, node 5 is a clusterhead marked as *L*0-5, which refers to the level of clustering (*L* = 0) and node ID (5).
- Similarly, each of the higher-level cluster leaders is also marked (*e.g.*, *L*1 − 6, *L* − 2 −6, and *L*3 − 6 refer to the same node 6, but acting as leader with the given leader IDsat levels 1, 2, and 3, respectively).
- The spectrum reuse schemes, including spreading code assignment, can be used among the cluster leaders of the *L* = 0 clusters. For the nodes under the leadership of node 6 at level 0, the cluster members are nodes 9, 10, 11, 12, and 17.
- Those nodes that belong to multiple clusters are referred to as cluster gateway nodes. For the level 0 cluster whose leader is node 6, the cluster gateways are nodes 10, 12, and 17.
- The second level of clustering is done among the leaders of the first level, that is, the leaders of 0*th* level clusters, *L*0 - 1, *L*0 - 2, *L0* - 3,*L0* - 4, *L0* - 5, and *L0* - 6, form the members of the first-level cluster.

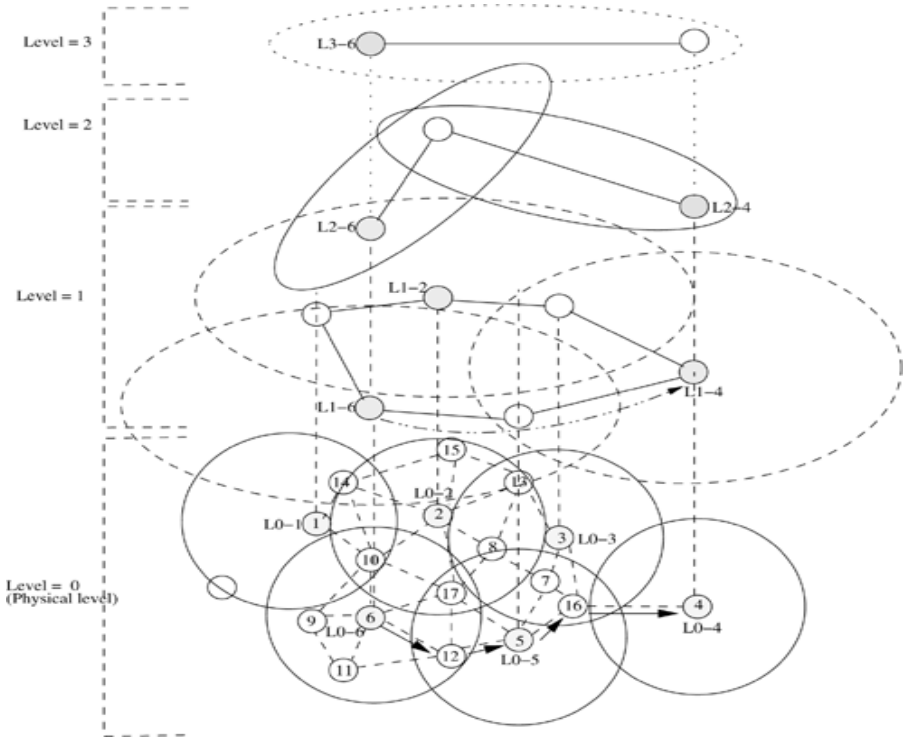


Figure 4.26. Example of HSR multi-level clustering.

Advantages

- Reduces routing table size storage required is O (n x m).
- For flat topology, it is O (nm)
  - n→ no. of nodes
  - m→ no. of levels

Disadvantage

- Process of exchanging information concerned all the levels of the hierarchy as well as theprocess of leader election in every cluster makes it quite problematic for adhoc networks.

4.6.2 Fish-Eye State Routing Protocol (FSR)

- It is a generalization of the GSR protocol.
- It uses Fisheye technique to reduce the routing overhead.
- Principle: Property of a fish's eye that can capture pixel information with greateraccuracy near its eye's focal point.
- This accuracy decreases with an increase in the distance from the center of the focal point
- This property is translated to routing in adhoc wireless networks by a node
- Each node maintains accurate information about near nodes.
- Nodes exchange topology information only with their neighbors.
- A sequence numbering scheme is used to identify the recent topology changes
- This constitutes a link-level information exchange of distance vector protocols andcomplete topology information exchange of link state protocols.
- FSR defines routing scope, which is the set of nodes that are reachable in a specific no. ofhops.
- The scope of a node at two hops is the set of nodes that can be reached in two hops fig
  4.27 shows scope of node 5 with one hop and two hops.
- The routing overhead is significantly reduced

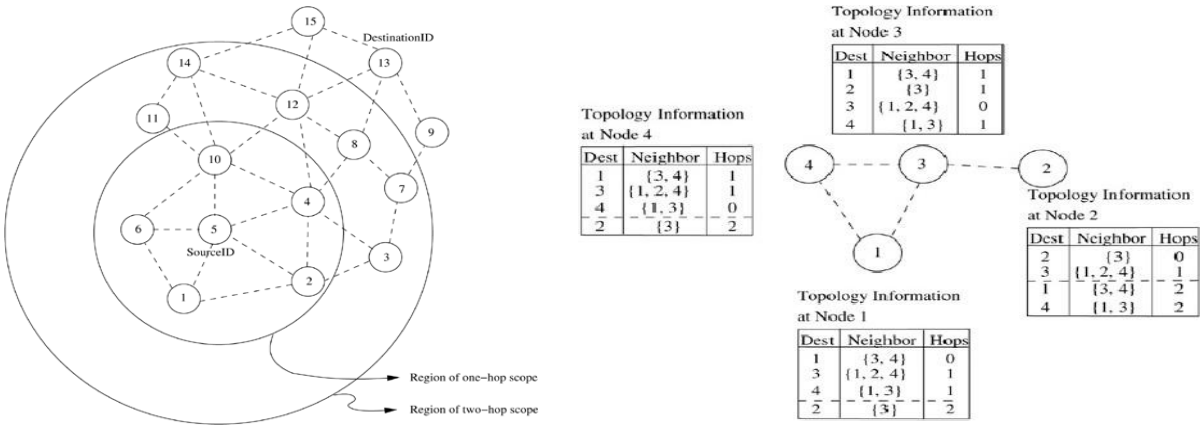


Figure 4.27. Fisheye state routing. Figure 4.28. An illustration of routing tables in FSR.

- The link state info for the nodes belonging to the smallest scope is exchanged at thehighest frequency. Frequency of exchanges decreases with an increase in scope.
- Fig 4.28 illustrates an example depicting the n/w topology information maintained atnodes in a n/w.
- Message size for a typical topology information update packet is significantly reduced.
- The routing information for the nodes that are one hop away from a node are exchanged more frequently than the routing information about nodes that are more than one hop away.
- Information regarding nodes that are more than one hop away from the current node are listed below the dotted line in the topology table.

Advantages

- Reduce bandwidth consumption by link state update packets.
- Suitable for large and highly mobile adhoc wireless network.

Disadvantage

- Very poor performance in small adhoc networks

4.7 Power-Aware Routing Protocols

Some of the Power-aware routing protocols are discussed below:

- ***Power-Aware Routing Metrics***

  The limitation on the availability of power for operation is a significant bottleneck. Hence, the use of routing metrics contributes to the efficient utilization of energy and increases the lifetime of the network

- ***Minimal energy consumption per packet***
  - This metric aims at minimizing the power consumed by a packet in traversing fromsource node to the destination node.
  - The energy consumed by a packet when traversing through a path is the sum of theenergies required at every intermediate hop in that path.
  - This metric doesn't balance the load;
    - **Disadvantages**
      - Selection of path with large hop length.
      - Inability to measure the power consumption in advance.
      - Inability to prevent the fast discharging of batteries at some nodes
- ***Maximize network connectivity***
  - This metric attempt to balance the routing load among the cut set (the subset

of thenodes in the network, the removal of which results in network partitions).

- It is difficult to achieve a uniform battery draining rate for the cut set.

- ***Maximum variance in Node power levels***
  - This metric proposes to distribute the load among all nodes in the network so thatthe power consumption pattern remains uniform across them.
  - This problem is very complex when the rate and size of the data packets vary

- ***Minimum cost per packet***
  - In order to maximize the life of every node in the network, this routing metric ismade as a function of the state of the node's battery.
  - A node's cost decreases with an increase in its battery change and vice versa.
  - Cost of node can be easily computed
    - **Advantage**
      - congestion handling & cost calculation

- ***Minimize maximum node cost***
  - This metric minimizes the maximum cost per node for a packet after routing a number ofpackets or after a specific period.
  - This delays the failure of a node, occurring due to higher discharge because of packetforwarding.