

## **UNIT – 3 ROUTING PROTOCOLS AND TRANSPORT LAYER IN**

### **AD HOC WIRELESS NETWORKS**

Since the ad hoc wireless network consists of a set of mobile nodes (hosts) that are connected by wireless links, the network topology in such a network may keep changing randomly. Hence a variety of routing protocols for ad hoc wireless networks has been proposed.

#### **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 ad-hoc 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 routing 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 ad-hoc 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.
- 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):

1. An improved version of MACA protocol.
2. Introduced to increase the efficiency.
3. 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 7.2.

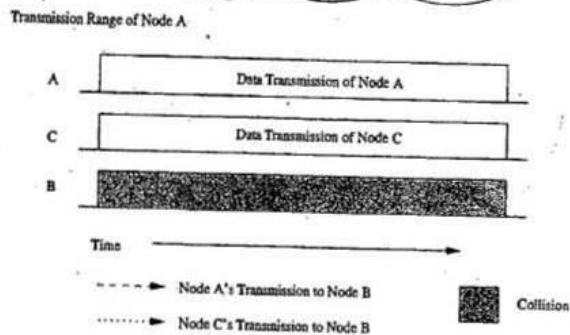
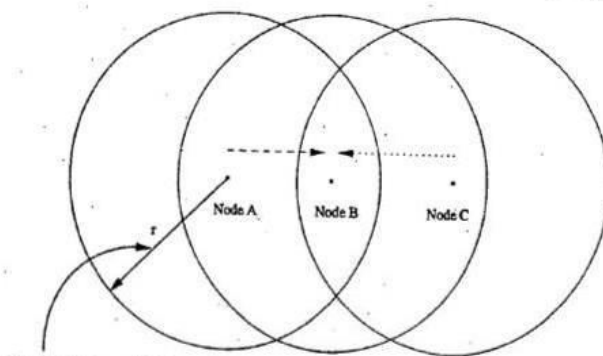


Figure 7.1. Hidden terminal problem.

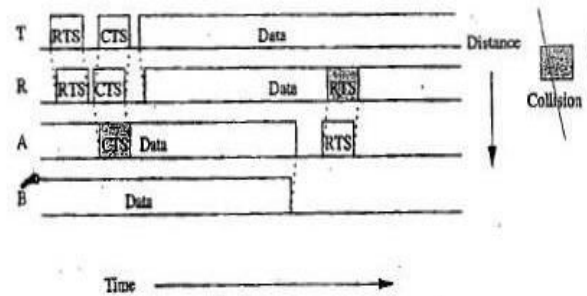
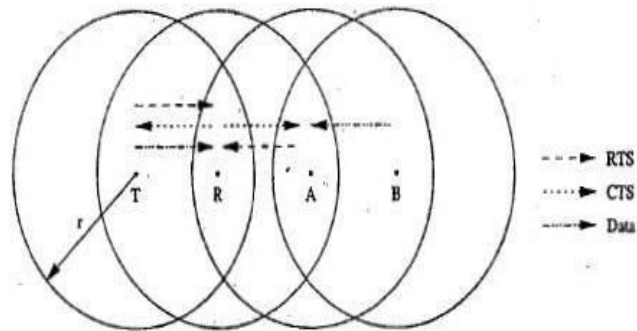


Figure 7.2. Hidden terminal problem with RTS-CTS-Data-ACK scheme.

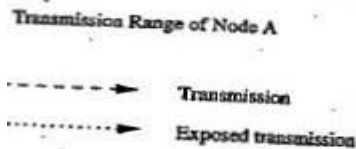
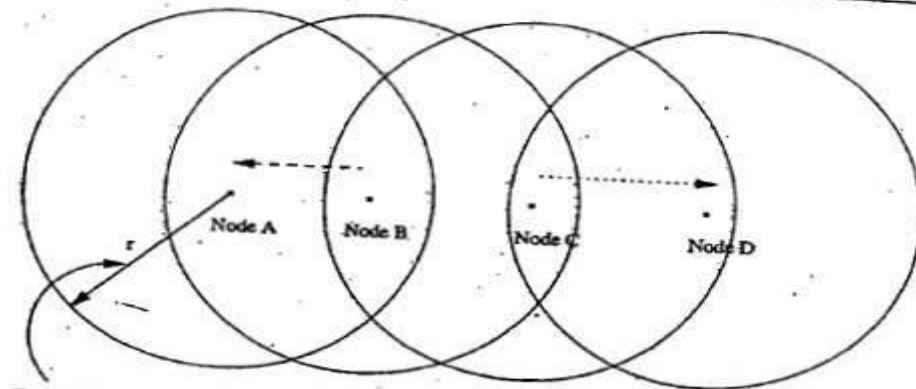


Figure 7.3. Exposed terminal problem.

## Resource Constraints

- Two essential and limited resources are battery life and processing power.
- Devices used in ad-hoc 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

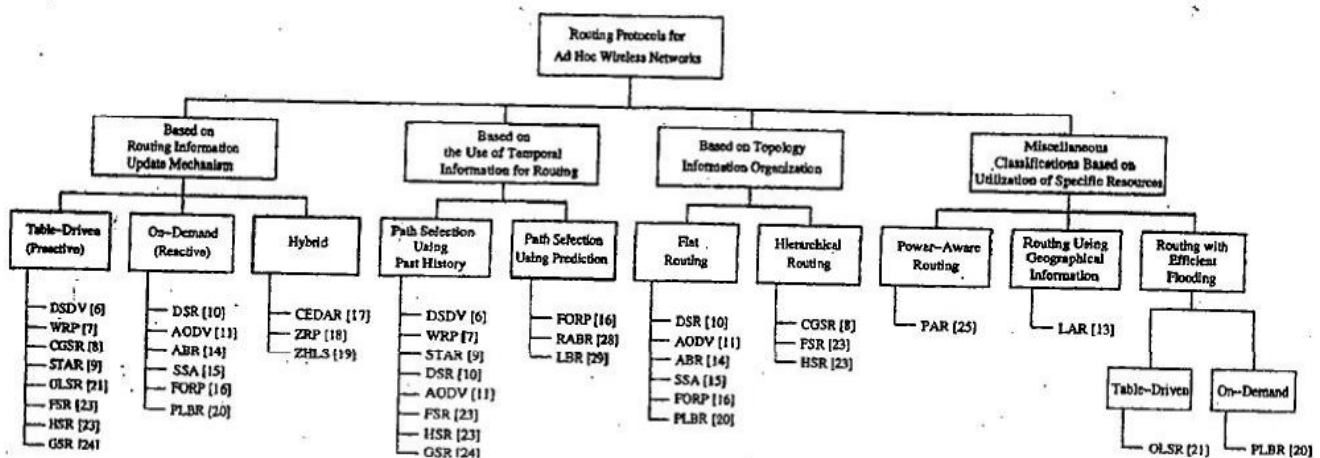


Figure 7.4. Classifications of routing protocols.

The routing protocol for ad-hoc 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.

## 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

- 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 (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 (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 ( $\infty$ ) and with a sequence number greater than the stored sequence number for that destination.
- Each node upon receiving an update with weight  $\infty$ , 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 7.6 shows the case when node 11 moves from its current position.

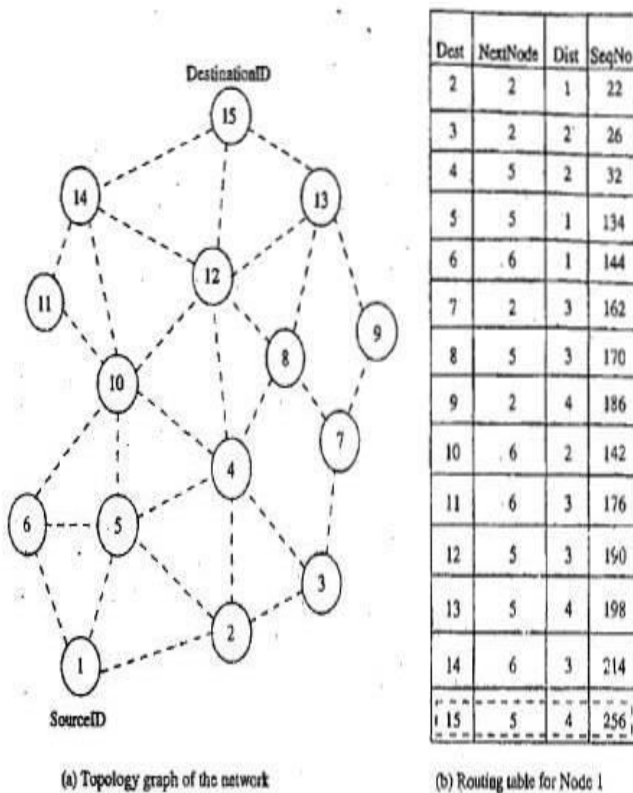


Figure 7.5. Route establishment in DSDV.

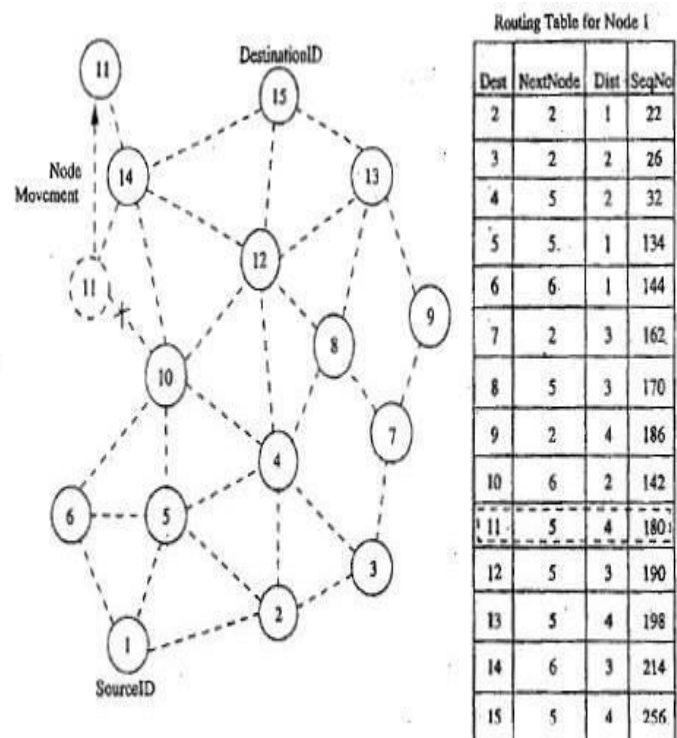


Figure 7.6. Route maintenance in DSDV.

### 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.

## 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  $\infty$ . 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.
- 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  $\infty$ . 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 7.8 shows route maintenance in WRP.

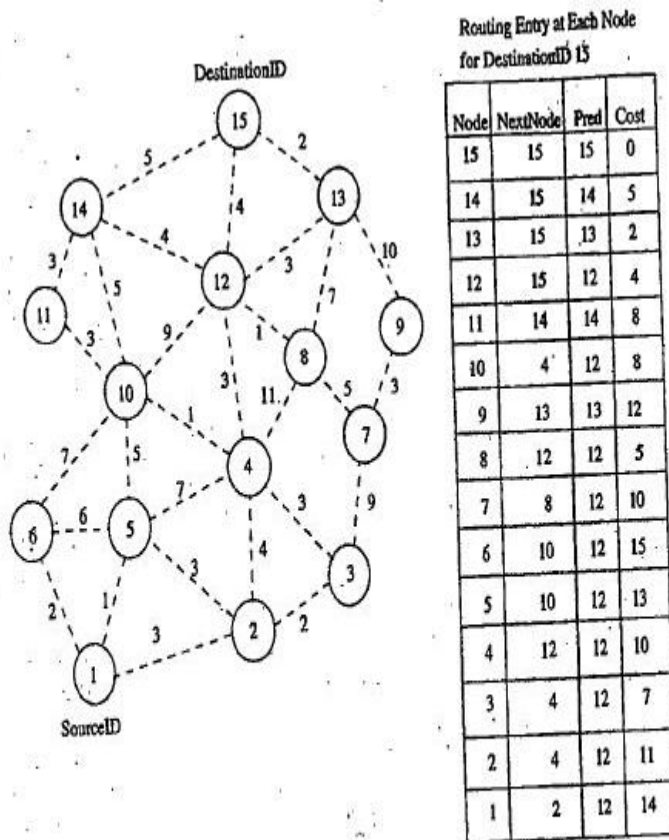


Figure 7.7. Route establishment in WRP.

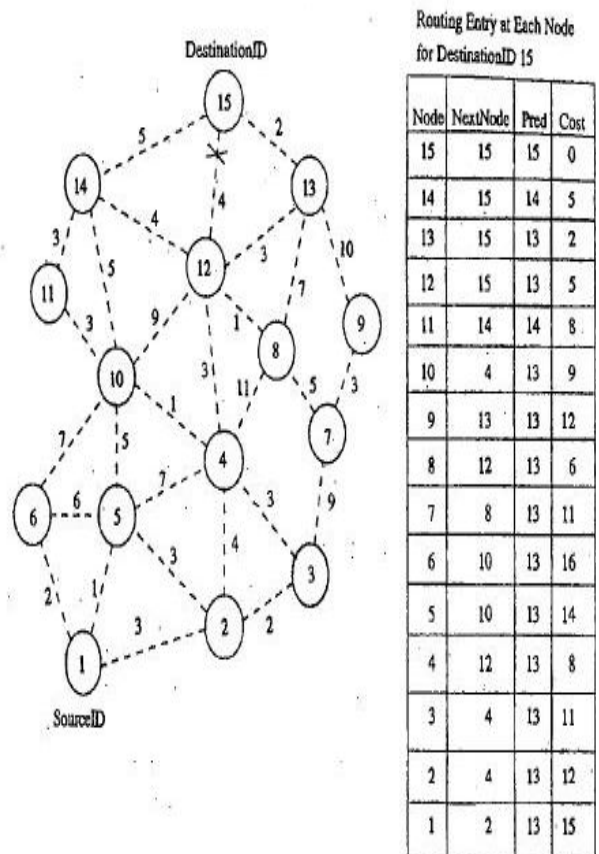


Figure 7.8. Route maintenance in WRP.

### 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.

## 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.
- CGSR 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 exist as a member.



- A gateway conflict is said to occur when a cluster-head issues a token to a gateway over spreading codewhile 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.

### Advantages

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

### Disadvantages

- Increase in path length and instability in the system at high mobility when the rate of change 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.

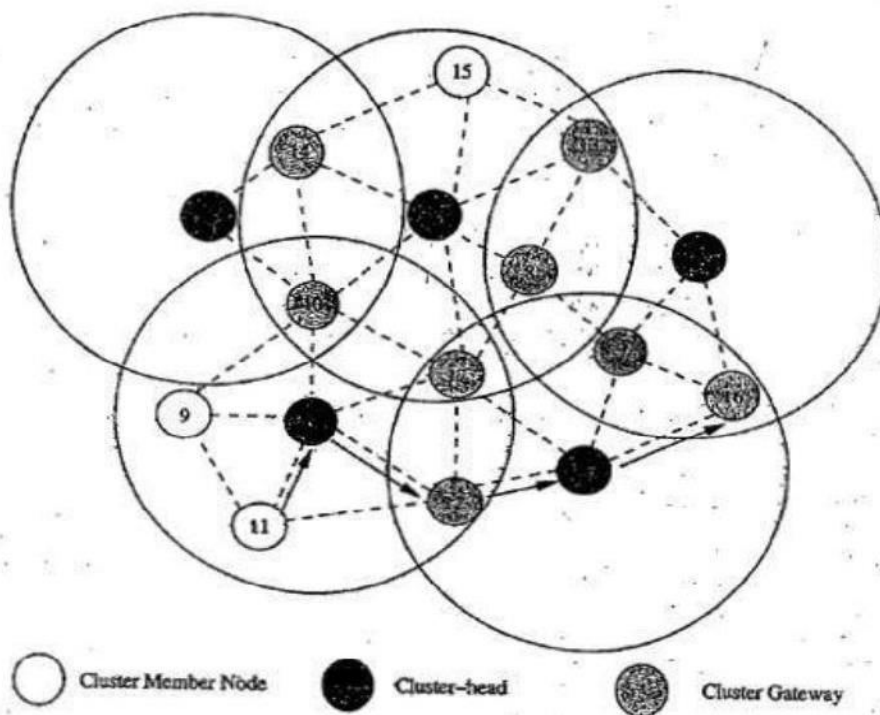


Figure 7.9. Route establishment in CGSR.



## Source-Tree Adaptive Routing Protocol (STAR)

- Key concept -least overhead routing approach (LORA)
- This protocol attempts to provide feasible paths that are not guaranteed to be optimal
- Involves much less control overhead
- In STAR protocol, every node broadcasts its source tree information
- The source tree of a node consists of the wireless links used by the node.
- Every node builds a partial graph of the topology.
- During initialization, a node sends an update message to its neighbors
- Each node will have a path to every destination node.
- The path would be sub-optimal.
- The data packet contains information about the path to be traversed in order to prevent the possibility of routing loop formation.
- In the presence of a reliable broadcast mechanism, STAR assumes implicit route maintenance.
- In addition to path breaks, the intermediate nodes are responsible for handling the routing loops
- The RouteRepair packet contains the complete source tree of node k and the traversed path of the packet.
- When an intermediate node receives a RouteRepair update message, it removes itself from the top of the route repair path and reliably sends it to the head of the route repair path.

### Advantages

- Very low communication overhead
- Reduces the average control overhead

## 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 Route Reply packet back to the source
- Each Route Request 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 7.10, 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.  
In fig 7.11, if the intermediate node 10 has a route to the destination via node 14, it also sends the RouteReply 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

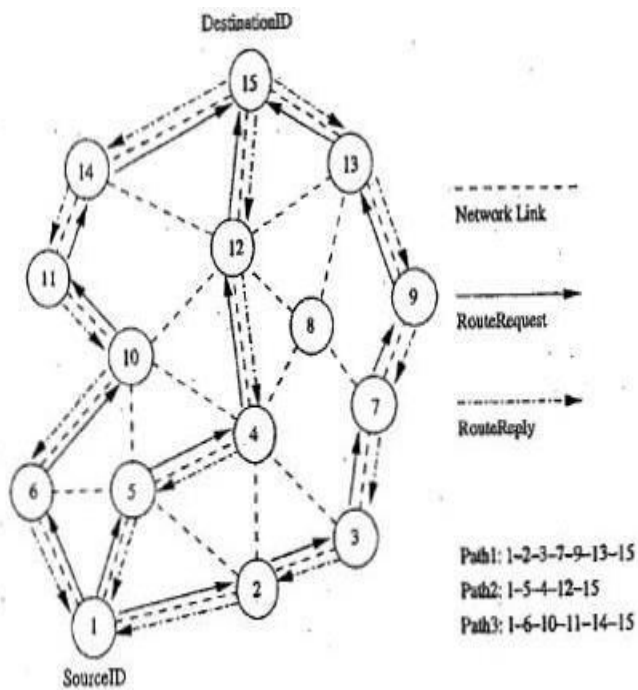


Figure 7.10. Route establishment in DSR.

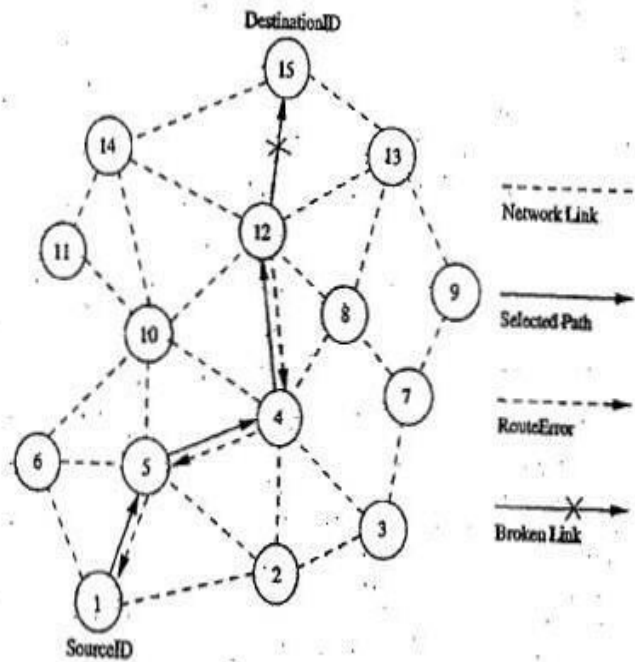


Figure 7.11. Route maintenance in DSR.

### 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.
- AODV does not repair a broken path locally

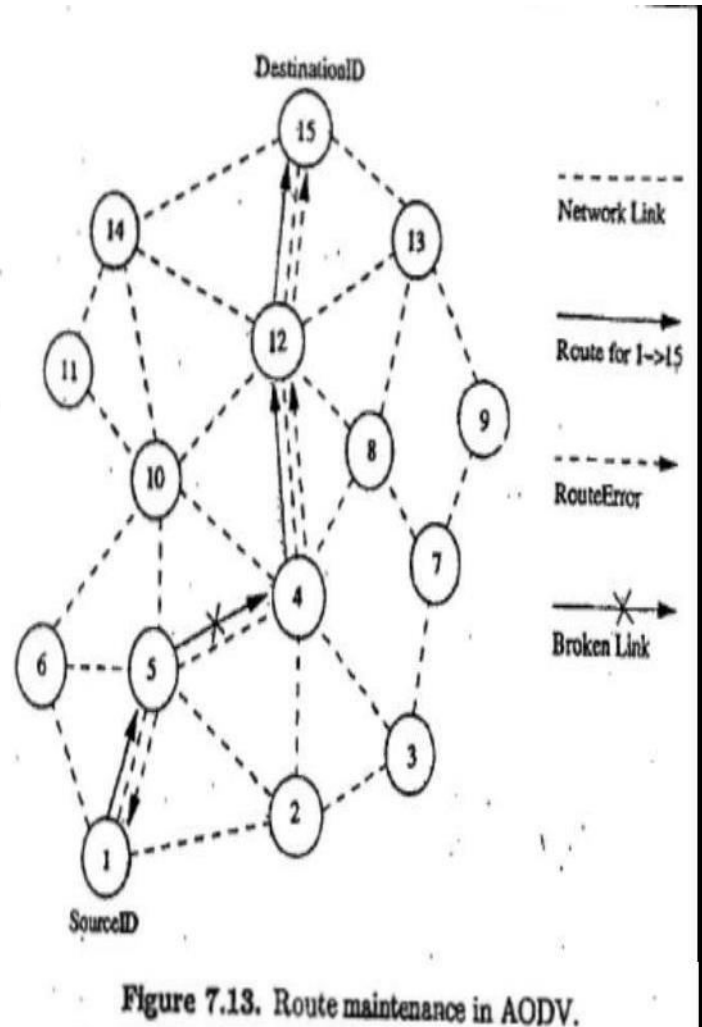
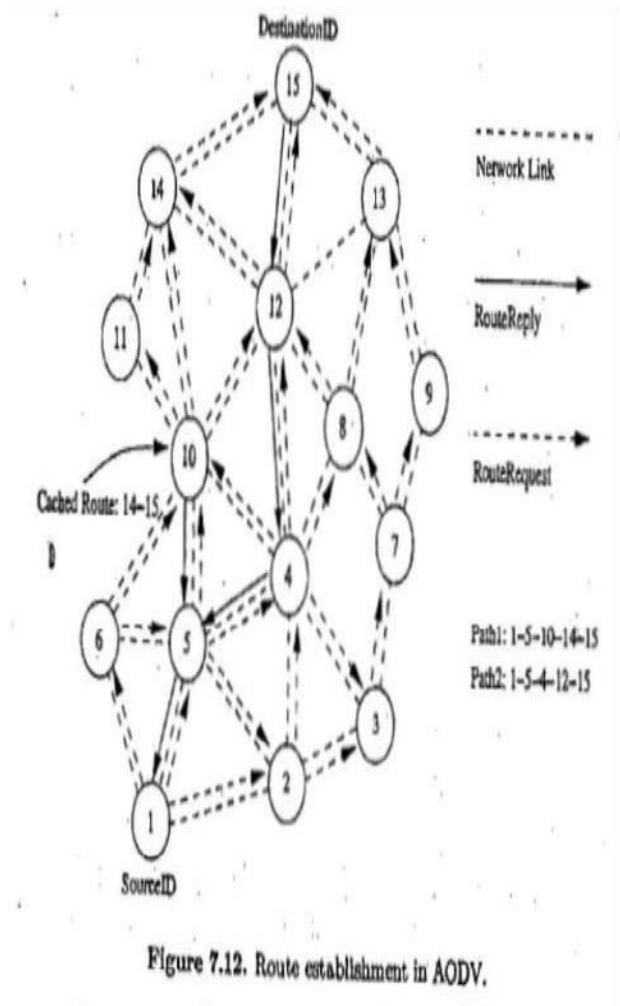
- When a link breaks, the end nodes are notified
- Source node re-establishes the route to the destination if required

### 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.



### Temporally Ordered Routing Algorithm (TORA)

- Source-initiated on-demand routing protocol.
- Uses a link reversal algorithm.
- Provides loop free multi path routes to the destination.
- Each node maintains its one-loop local topology information.
- Has capability to detect partitions.
- Unique property limiting the control packets to a small region during the reconfiguration process initiated by a path break

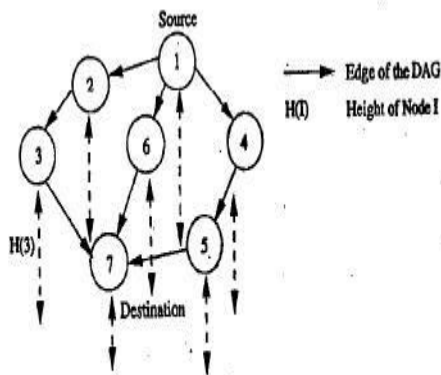


Figure 7.14. Illustration of temporal ordering in TORA.

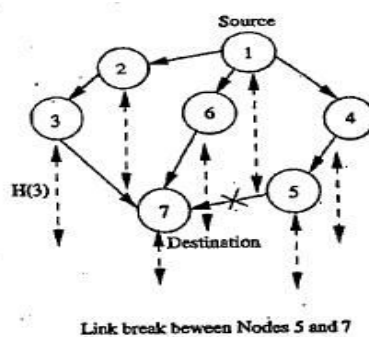
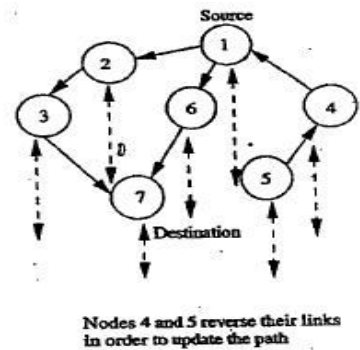


Figure 7.15. Illustration of route maintenance in TORA.



- TORA has 3 main functions: establishing, maintaining and erasing routes
- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link.
- This process establishes a destination-oriented directed acyclic graph using a query/update mechanism.
- Once the path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the re-configurations that may take place during the course of data transfer session
- If the node detects a partition, it originated a clear message, which erases the existing path information in that partition related to the destination.

#### Advantages

- Incur less control overhead
- Concurrent detection of partitions
- Subsequent deletion of routes

#### Disadvantages

- Temporary oscillations and transient loops
- Local reconfiguration of paths result in non-optimal routes

#### Location-Aided Routing (LAR)

- It utilizes the location information for improving the efficiency of routing by reducing the control overhead
- LAR assumes the availability of the global positioning system (GPS) for obtaining the geographical position information necessary for routing.
- LAR designates two geographical regions for selective forwarding of control packets, namely, ExpectedZone and RequestZone.
- The ExpectedZone is the region in which the destination node is expected to be present, given information regarding its location in the past and its mobility information.
- The RequestZone is a geographical region within which the path-finding control packets are permitted to be propagated.
- This area is determined by the sender of a data transfer session.
- The control packets used for path-finding are forwarded by nodes which are present in the RequestZone and are discarded by nodes outside the zone.
- LAR uses flooding, but here flooding is restricted to a small geographical region.
- The nodes decide to forward or discard the control packets based on two algorithms, namely, LAR1 & LAR2

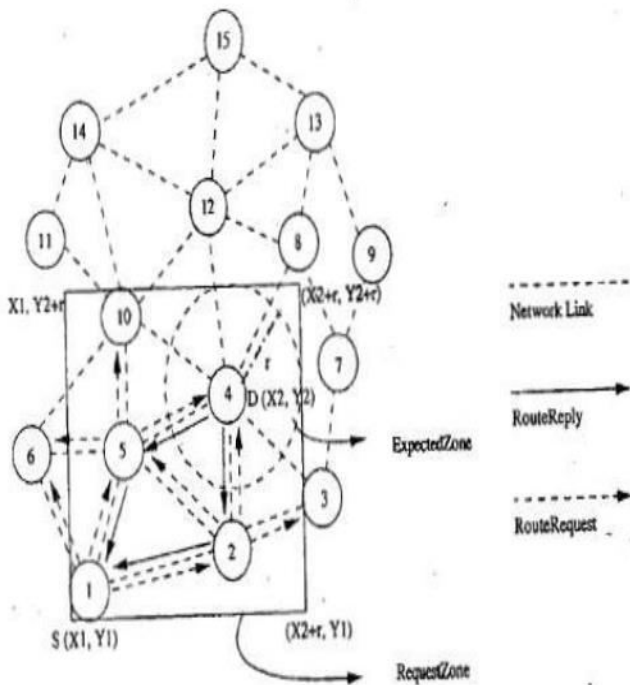


Figure 7.16. RequestZone and ExpectedZone in LAR1.

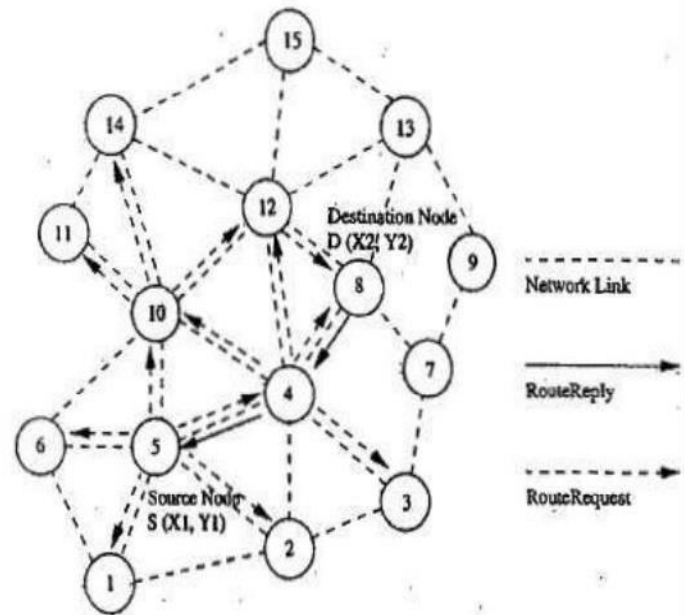


Figure 7.17. Route establishment in LAR2.

- In the LAR1 algorithm (fig 7.16), the source node explicitly specifies the RequestZone in the RouteRequest packet which is broadcast to its neighbors.
- These nodes verify their own geographical locations to check whether they belong to the ExpectedZone.
- Finally, when the RouteRequest reaches the destination node, it originates a RouteReply that contains the current location and current time of the node.
- In LAR2 algorithm (fig 7.17), the source node includes the distance between itself and the destination node.
- When the intermediate node receives this RouteRequest packet, it computes the distance to the node D.
- A RouteRequest packet is forwarded only once and the distance between the forwarding node and D is updated in the RouteRequest packet for further relaying.
- In order to compensate for the location error, a larger RequestZone that can accommodate the amount of error that occurred is considered

#### Advantage

- LAR reduces the control overhead by limiting the search area for finding a path.
- Efficient use of geographical position information.
- Reduced control overhead.
- Increased utilization of bandwidth.

#### Disadvantage

- Depends heavily on the availability of GPS infrastructure.
- Hence, cannot be used in situations where there is no access to such information

#### Associativity-Based Routing (ABR)

- It is a distributed routing protocol that selects routes based on the stability of the wireless links.
- It is a beacon-based on-demand routing protocol.
- A link is classified as stable or unstable based on its temporal stability.
- The temporal stability is determined by counting the periodic beacons that a node receives from its neighbors.
- Each node maintains the count of its neighbor's beacons and classifies each link as stable or unstable.

- The link corresponding to a stable neighbor is termed as a stable link, while a link to an unstable neighbor is called an unstable link.
- A source node floods RouteRequest packets throughout the network if a route is not available in its route cache.
- All intermediate nodes forward the RouteRequest packet.
- RouteRequest packet carries the path it has traversed and the beacon count for the corresponding nodes in the path.
- When the first RouteRequest reaches the destination, the destination waits for a time period T to receive multiple RouteRequests through different paths.
- If two paths have the same proportion of stable links, the shorter of them is selected.
- If more than one path is available, then a random path among them is selected as the path between source and destination.

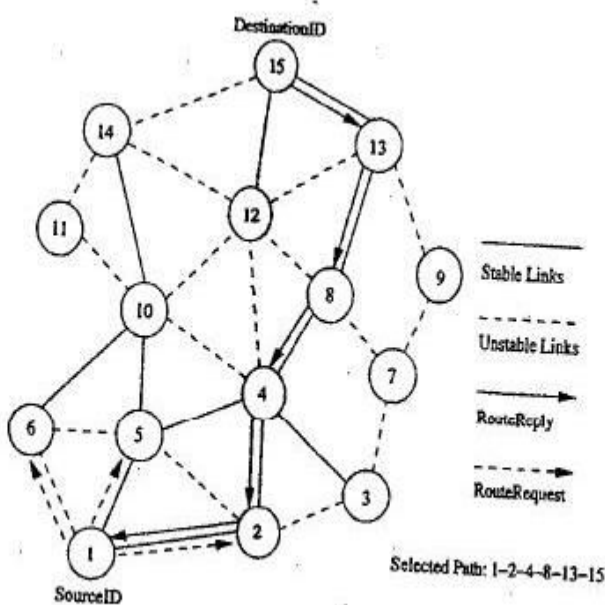


Figure 7.18. Route establishment in ABR.

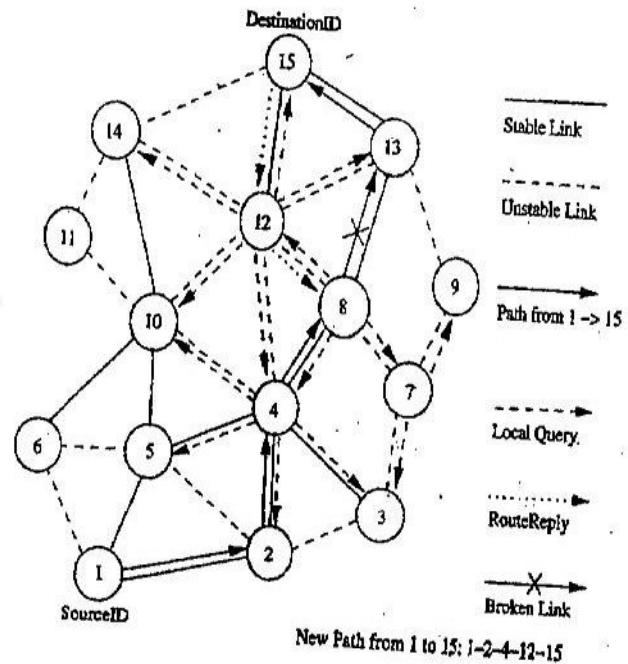


Figure 7.19. Route maintenance in ABR.

In figure 7.18, source node initiates the RouteRequest to the flooded for finding a route to the destination node

- Solid lines represent stable links.
- Dotted lines represent unstable links.
- ABR uses stability information only during the route selection process at the destination node.
- If a link break occurs at an intermediate node, the node closer to the source, which detects the break, initiates a local route repair process.
- In this process, the node locally broadcasts a route repair packet, termed the local query (LQ) broadcast, with a limited time to live (TTL), as shown in figure 7.19.
- This way a broken link is bypassed locally without flooding a new RouteRequest packet in the whole network.

#### Advantage

- Stable routes have a higher preference compared to shorter routes
- They result in fewer path breaks which, in turn, reduces the extent of flooding due to reconfiguration of paths in the network

## Disadvantage

- Chosen path may be longer than the shortest path between the source and destination because of the preference given to stable paths.
- Repetitive LQ broadcasts may result in high delays during route repairs

## Signal Stability-Based Adaptive Routing Protocol (SSA)

- Uses signal stability as the prime factor for finding stable routes.
- This protocol is beacon-based, in which signal strength of the beacon is measured for determining link stability.
- The signal strength is used to classify a link as stable or unstable.
- This protocol consists of two parts: forwarding protocol (FP) and dynamic routing protocol (DRP).
- These protocols use an extended radio interface that measures the signal strength from beacons.
- DRP maintains the routing table by interacting with the DRP processes on other hosts.
- FP performs the actual routing to forward a packet on its way to the destination.
- Every node maintains a table that contains the beacon count and the signal strength of each of its neighbors.
- If a node receives strong beacons, then link is classified as strong/stable link.
- The link is otherwise classified as weak/unstable link.
- Each node maintains a table called the signal stability table (SST) which is based on the signal strengths of its neighbors' beacons.
- This table is used by the nodes in the path to the destination to forward the incoming RouteRequest over strong links for finding the most stable end-to-end path.
- A source node which does not have a route to the destination floods the network with RouteRequest packets.
- SSA protocol process a RouteRequest only if it is received over a strong link.
- A RouteRequest received through a weak link is dropped without being processed.
- The destination selects the first RouteRequest packet received over strong links.
- The destination initiates a RouteReply packet to notify the selected route to the source.
- In figure 7.20, source node broadcasts a RouteRequest for finding the route to the destination node.
- Solid lines represent the stable links.
- Dotted lines represent the weak links.
- SSA restricts intermediate nodes from forwarding a RouteRequest packet if the packet has been received over a weak link.
- When a link breaks, the end nodes of the broken link notify the corresponding end nodes of the path.
- A source node, after receiving a route break notification packet, rebroadcasts the RouteRequest to find another stable path to the destination.
- Stale entries are removed only if data packets that use the stale route information fail to reach the next node.
- If no strong path is available when a link gets broken, then the new route is established by considering weak links also.
- This is done when multiple RouteRequest attempts fail to obtain a path to the destination using only the stable links.

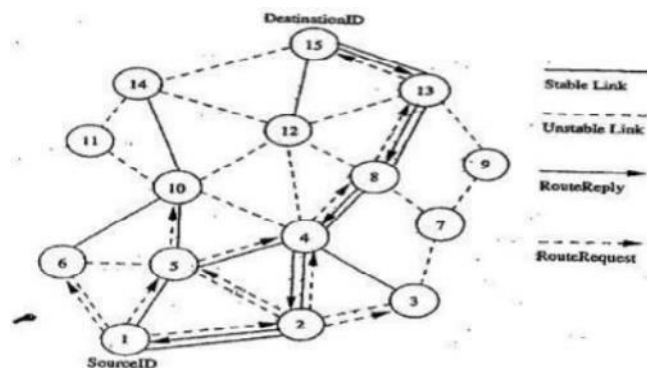


Figure 7.20. Route establishment in SSA.



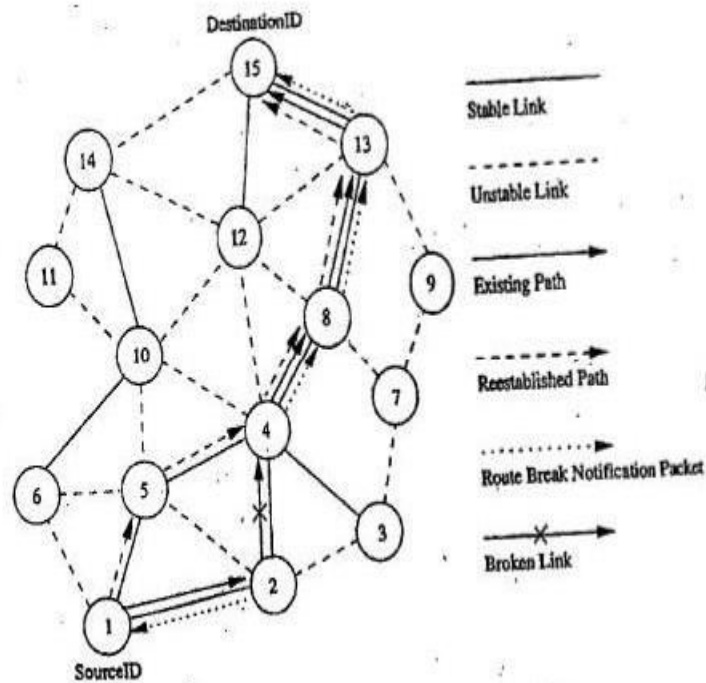


Figure 7.21. Route maintenance in SSA.

### Advantage

- Finds more stable routes when compared to the shortest path route selection protocols.
- Accommodates temporal stability by using beacon counts to classify a link as stable or weak

### Disadvantage

- It puts a strong RouteRequest forwarding condition which results in RouteRequest failures.
- Multiple flooding of RouteRequest packets consumes significant amount of bandwidth.
- Increases the path setup time.
- Strong link criterion increases the path length

### Flow-Oriented Routing Protocol (FORP)

- Employs a prediction-based multi-hop-handoff mechanism for supporting time-sensitive traffic in adhoc wireless networks.
- Proposed for IPv6-based ad hoc wireless networks where QoS needs to be provided.
- The multi-hop-handoff is aimed at alleviating the effects of path breaks on the real time packet flows.
- A sender or an intermediate node initiates the route maintenance process only after detecting a link break.
- It may result in high packet loss leading to a low QoS provided to the user.
- FORP utilizes the mobility and location information of nodes to estimate the link expiration time (LET).
- LET is the approximate lifetime of a given wireless link.
- The minimum of the LET values of all wireless links on a path is termed as the route expiry time (RET).
- Every node is assumed to be able to predict the LET of each of its links with its neighbors.
- The LET between two nodes can be estimated using information such as current position of the nodes, their direction of movement, and their transmission ranges.
- FORP requires the availability of GPS information in order to identify the location of nodes.
- When a sender node needs to setup a real time flow to a particular destination, it checks its routing table for the availability of a route to that destination.
- If a route is available, then that is used to send packets to the destination.
- Otherwise sender broadcasts a flow-REQ packet carrying information regarding the source and destination nodes.
- The Flow-REQ packet also carries a flow identification number/sequence number which is unique for every session

- A neighbor node, on receiving this packet, first checks if the sequence number of the received Flow-REQ is higher than the sequence number corresponding to previous packet.
- If the sequence number on the packet is less than that of the previous packet, then the packet is discarded.
- This is done to avoid looping of flow-REQ packets.
- The Flow-REQ packet, when received at the destination node, contains the list of nodes on the path it had traversed, along with the LET values of every wireless link on that path.
- FORP assumes all the nodes in the network to be synchronized to a common time by means of GPS Information.

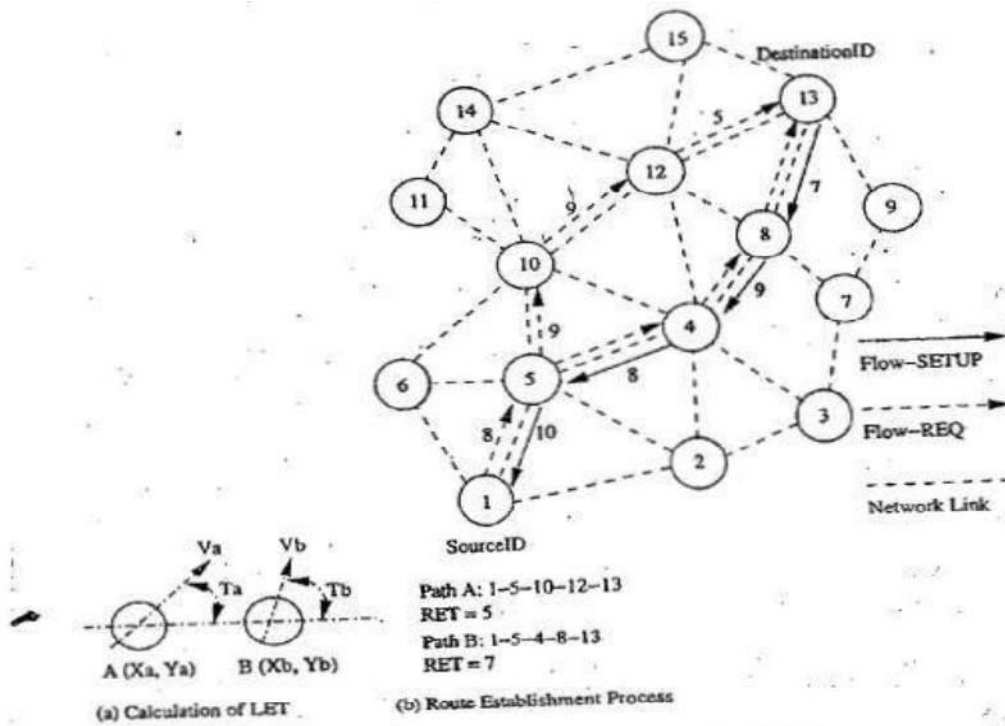


Figure 7.22. Route establishment in FORP.

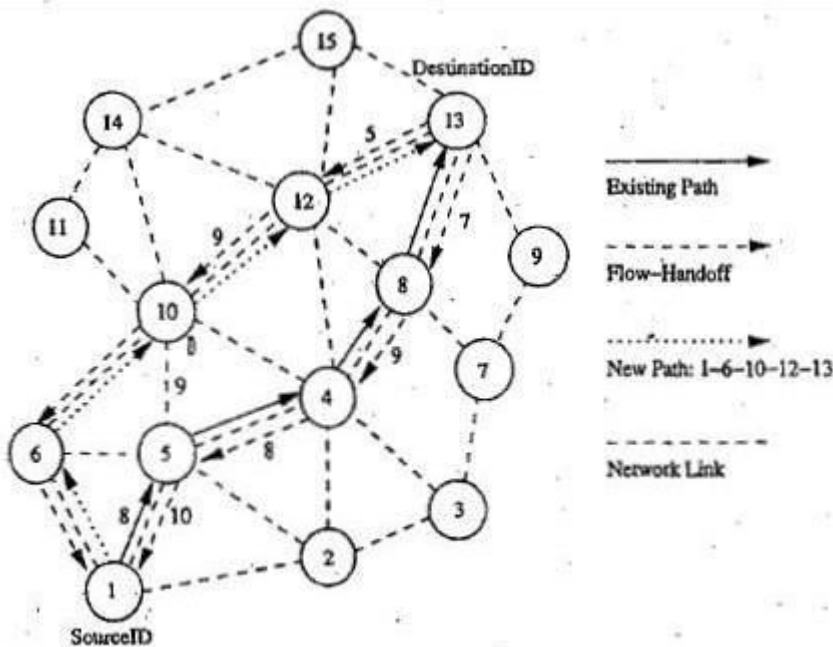


Figure 7.23. Route maintenance in FORP.

### Advantage

- Use of LET and RET estimates reduces path breaks
- Reduces the reduction in packet delivery.
- Reduces number of out-of-order packets.
- Reduces non-optimal paths

### Disadvantage

- Works well when topology is highly dynamic.
- Requirements of time synchronization increases the control overhead.
- Dependency on GPS infrastructure affects the operability of this protocol wherever it is not available

## 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 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 chose

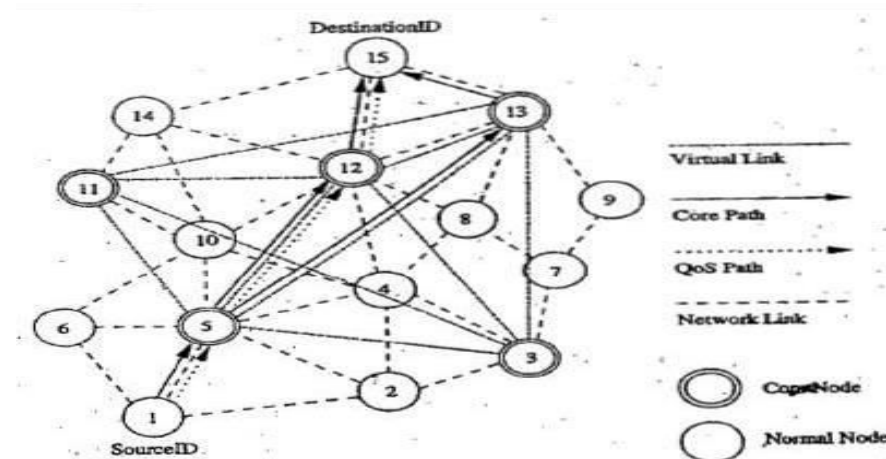


Figure 7.24. Route establishment in CEDAR.

- Route Maintenance in CEDAR: attempts to repair a broken route locally when a path break occurs.
- A node after which the break occurred:
  1. Sends a notification of failure.
  2. Begins to find a new path from it to the destination.
  3. Rejects every received packet till the moment it finds the new path to the destination.
- Meanwhile, as the source receives the notification message:
  1. It stops to transmit.
  2. Tries to find a new route to the destination.
  3. If the new route is found by either of these two nodes, a new path from the source to the destination is established.

### 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).
- 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.

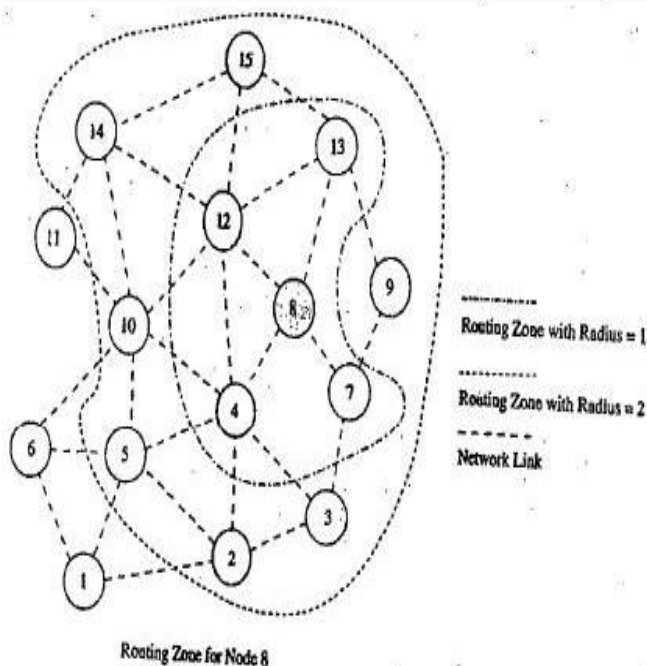


Figure 7.26. Routing zone for node 8 in ZRP.

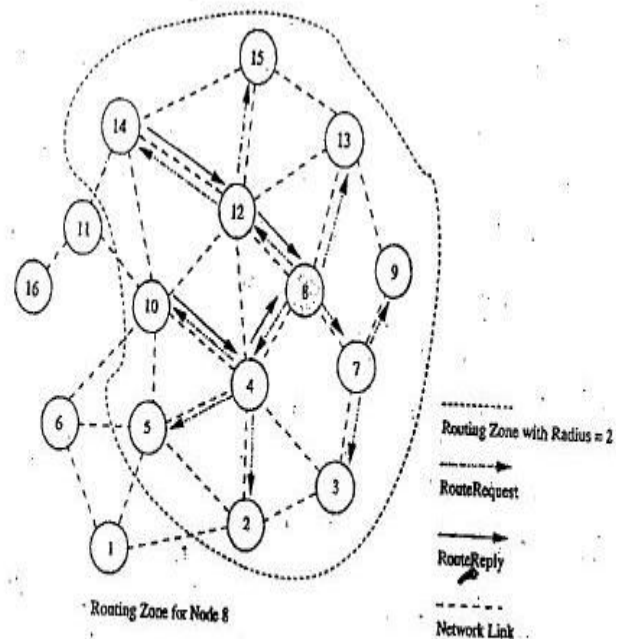


Figure 7.27. Path finding between node 8 and node 16.

**Route Establishment:** When a node *s* (node 8 in the fig 7.27) 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 rebroadcasts 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.

### Advantage

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

### Disadvantage

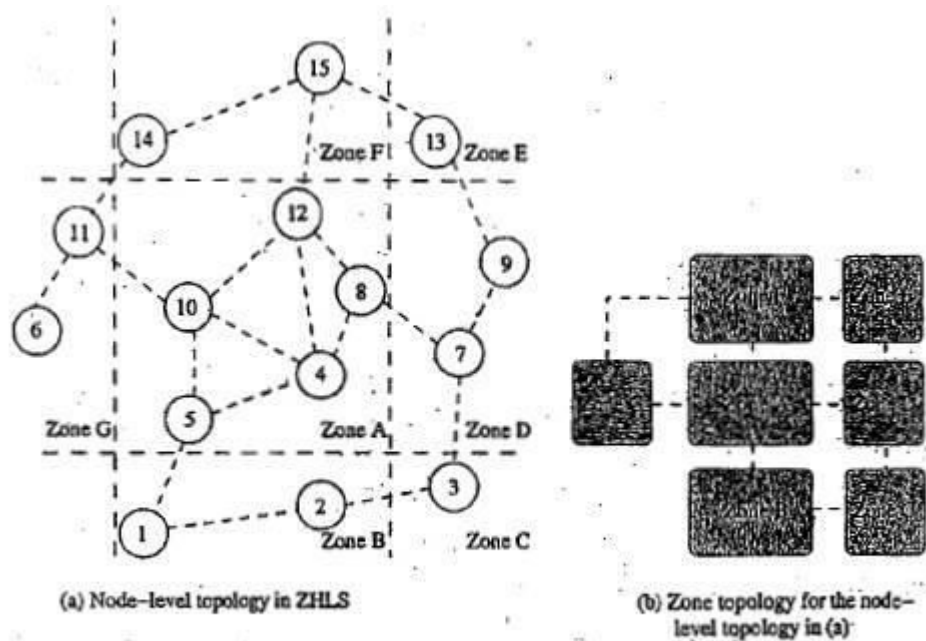
Control overhead may increase due to the large overlapping of nodes routing zones.

## Zone Based Hierarchical Link State Routing Protocol (ZHLS)

- ZHLS uses the geographical location info of the nodes to form non-overlapping zones. A Hierarchical 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 zone and a Reactive approach behind the zone.
- Every node requires GPS support for obtaining its own geographical location that is used to map itself into corresponding zone.
- The assignment of zone addresses to geographical areas is important and is done during a phase called the network design phase or network deployment phase.
- Each node maintains two link state packets: (LSP)
- Node level LSP: list of connected neighbors.
- 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.

**Table 7.1: Zone link state packets**

Source Zone	Zone Link State Packet
A	B, D, E, 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 7.28.** Zone-based hierarchical link state routing protocol.

**Route Maintenance** -If a given gateway node away causing a zone level connection failure, routing can still take 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.

#### Advantages

- Reduce storage requirements and common overhead.
- Robust and resilient to path breaks.
- Non overlapping zones.

#### Disadvantages

- Additional overhead incurred in creation of zone level topology.
- Path to Destination is suboptimal.
- Geographical info may not be available in all environments.

## ISSUES IN DESIGNING A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

### 1. Induced Traffic:

- In a path having multiple link, the traffic at any given link (or path) due to the traffic through neighboring links (or paths) is referred to as induced traffic.
- This is due to the broadcast nature of the channel and the location-dependent contention on the channel.
- Induced Traffic affects the throughput achieved by the transport layer protocol.

### 2. Induced throughput unfairness:

- This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layer such as the n/w and MAC layers.
- A transport layer should consider these in order to provide a fair share of throughput across contending flows

### 3. Separation of congestion control, reliability and flow control:

- A transport layer protocol can provide better performance if end-to-end reliability, flow control and congestion control are handled separately.
- Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity
- Objective : minimization of the additional control overhead generated by them

### 4. Power and Band width constraints:

- Nodes in ad hoc wireless networks face resource constraints including the two most important resources: (i) power source and (ii) bandwidth.
- The performance of a Transport layer protocol is significantly affected by these resource constraints

#### **5. Interpretation of congestion:**

- Interpretation of network congestion as used in traditional networks is not appropriate in ad hoc networks.
- This is because the high error rates of wireless channel, location-dependent contention, hidden terminal problem, packet collisions in the network, path breaks due to mobility of nodes, and node failure due to drained battery can also lead to packet loss in ad hoc wireless networks

#### **6. Completely decoupled transport layer:**

- Another challenge faced by Transport layer protocol is the interaction with the lower layers.
- Cross-layer interaction between the transport layer and lower layers is important to adapt to the changing network environment

#### **7. Dynamic topology:**

- Experience rapidly changing network topology due to mobility of nodes.
- Leads to frequent path breaks, partitioning and remerging of networks & high delay in reestablishment of paths
- Performance is affected by rapid changes in network topology.

### **DESIGN GOALS OF A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS**

- The protocol should maximize the throughput per connection.
- It should provide throughput fairness across contending flows.
- It should incur minimum connection set up and connection maintenance overheads.
- It should have mechanisms for congestion control and flow control in the network.
- It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
- It should be able to adapt to the dynamics of the network such as rapid changes in topology.
- Bandwidth must be used efficiently.
- It should be aware of resource constraints such as battery power and buffer sizes and make efficient use of them.
- It should make use of information from the lower layers for improving network throughput.
- It should have a well-defined cross-layer interaction framework.
- It should maintain End-to-End Semantics.