Routing Protocols for Ad Hoc Mobile Wireless Networks

Padmini Misra, misra@cis.ohio-state.edu

http://www.cis.ohio-state.edu/~misra

Abstract

The routing protocols meant for wired networks can not be used for mobile ad hoc networks because of the mobility of networks. The ad hoc routing protocols can be divided into two classes :- table-driven and on-demand. This paper discusses routing protocols belonging to each category.

See Also: TCP Extensions for Wireless Networks | Evolution Toward Third Generation Wireless Networks | In-building Wireless LAN | Wireless ATM - An Overview (slides)| The Wireless LANs Page | A Survey on Mobile IP | Mobile Computing & Disconnected Operation | Wireless Data Networking (slides)| Wireless Data Networking and Mobile Computing | Wireless Networking and Mobile IP References | Books on Wireless Networking and Mobile IP |
Other Reports on Recent Advances in Networking
Back to Raj Jain's Home Page

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

Table of Contents:

1. Introduction

Wireless networks is an emerging new technology that will allow users to access information and services electronically, regardless of their geographic position. Wireless networks can be classified in two types:- infrastructured network and infrastructureless (ad hoc) networks. Infrastructured network consists of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed.

In contrast to infrastructure based networks, in ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain[Royer99].

This article discusses proposed routing protocols for these ad hoc networks. These routing protocols can be divided into two categories: table-driven and on-demand routing based on when and how the routes are discovered. In table driven routing protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host. Next two sections discuss current table-driven protocols as well as on-demand protocols.

[Back to Table of Contents]

2. Table Driven Routing Protocols

In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain a consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1 Dynamic Destination-Sequenced Distance-Vector Routing Protocol

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm [Perkins94] is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements.

Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways:- a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent. Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon.

2.2 The Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) [Murthy96] is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor.

Node exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of update message (formed using MRL) are required to acknowledge the receipt of update message. If there is no change in routing table since last update, the

node is required to send an idle Hello message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables. The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a change in link of any of its neighbors. Consistency check in this manner helps eliminate looping situations in a better way and also has fast convergence.

2.3 Global State Routing

Global State Routing (GSR)[Chen98] is similar to DSDV described in section 2.1. It takes the idea of link state routing but improves it by avoiding flooding of routing messages.

In this algorithm, each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors.). For each destination node, the Topology table contains the link state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors.

2.4 Fisheye State Routing

Fisheye State Routing (FSR) [Iwata99] is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from node increases. Figure 1 defines the scope of fisheye for the center (red) node. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination. FSR scales well to large networks as the overhead is controlled in this scheme.
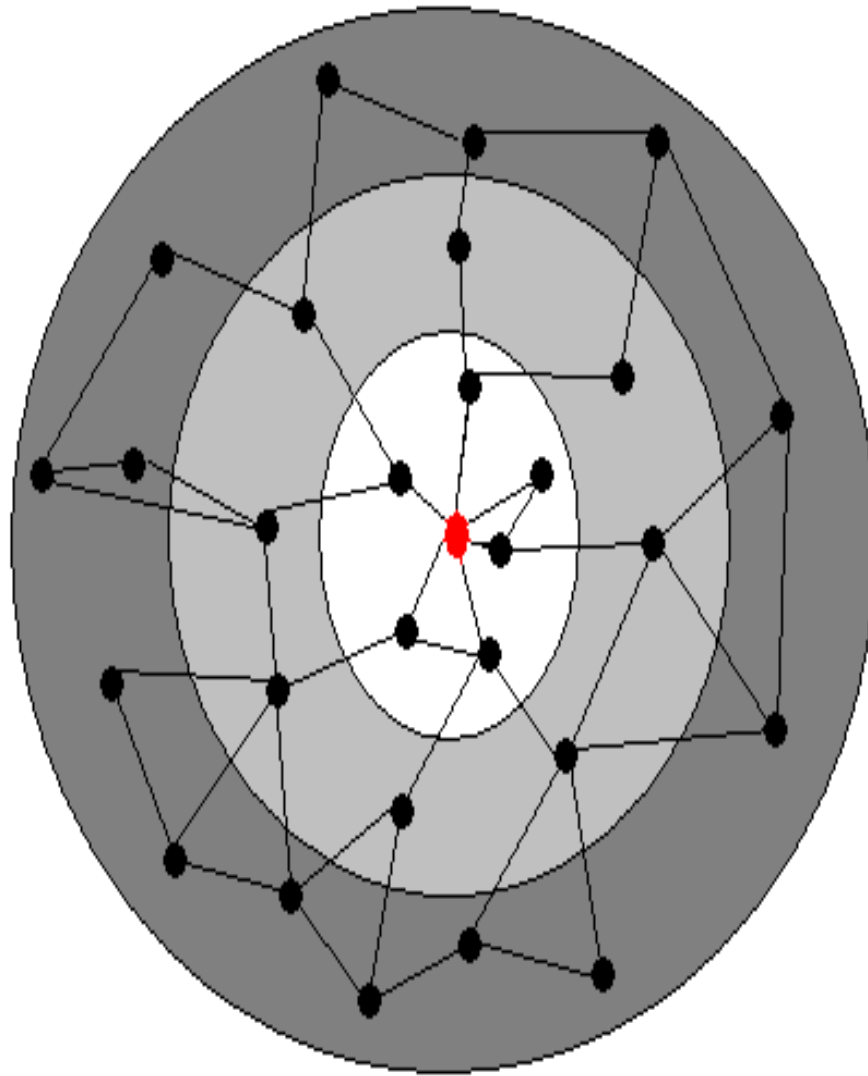
Figure 1. Accuracy of information in FSR

2.5 Hierarchical State Routing

The characteristic feature of Hierarchical State Routing (HSR) [Iwata99] is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. The nodes of a phyrical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighboring cluster-heads via gateway (section 2.2). As shown in the figure 2, these cluster-heads are member of the cluster on a level higher and they exchange their link information as well as the summarized lower-level information among each other and so on. A node at each level floods to its lower level the information that it obtains after the algorithm has run at that level. So the lower level has a hierarchical topology information. Each node has a hierarchical address. One way to assign hierarchical address is the cluster numbers on the way from root to the node as shown in figure 2. A gateway can be reached from the root via more than one path, so gateway can have more than one hierarchical address. A hierarchical address is enough to ensure delivery from anywhere in the network to the host.
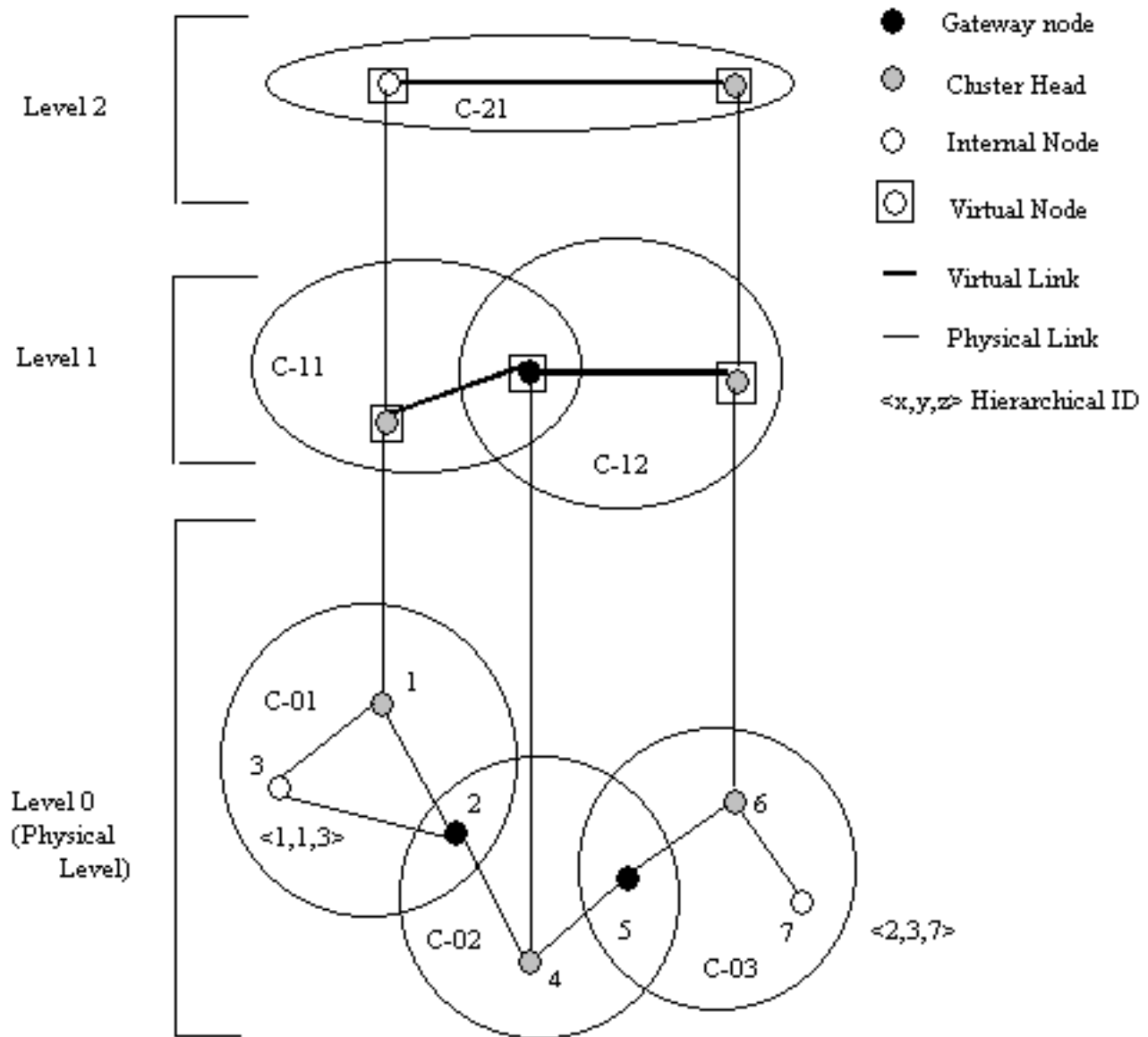
Figure 2. An example of clustering in HSR

In addition, nodes are also partitioned into logical subnetworks and each node is assigned a logical address <subnet, host>. Each subnetwork has a location management server (LMS). All the nodes of that subnet register their logical address with the LMS. The LMS advertise their hierarchical address to the top levels and the information is sent down to all LMS too. The transport layer sends a packet to the network layer with the logical address of the destination. The network layer finds the hierarchical address of the hierarchical address of the destinationÆs LMS from its LMS and then sends the packet to it. The destinationÆs LMS forwards the packet to the destination. Once the source and destination know each otherÆs hierarchical addresses, they can bypass the LMS and communicate directly. Since logical address/hierarchical address is used for routing, it is adaptable to network changes.

2.6 Zone-based Hierarchical Link State Routing Protocol

In Zone-based Hierarchical Link State Routing Protocol (ZHLS)[Joa-Ng99], the network is divided into non-overlapping zones. Unlike other hierarchical protocols, there is no zone-head. ZHLS defines two levels of topologies - node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some node of the other zone. Zone level topology tells how zones are connected together. There are two types of Link State Packets (LSP) as well - node LSP and zone LSP. A node LSP of a node contains its neighbor node information and is propagated with the zone where as a zone LSP contains the zone information and is propagated globally. So each node has full node connectivity knowledge about the nodes in its zone and only zone connectivity information about other zones in the network. So given the zone id and the node id of a destination, the packet is routed based on the zone id till it reaches the correct zone. Then in that zone, it is routed based on node id. A <zone id, node id> of the destination is sufficient for routing so it is adaptable to changing topologies.

2.7 Clusterhead Gateway Switch Routing Protocol

Clusterhead Gateway Switch Routing (CGSR) [Chiang97] uses as basis the DSDV Routing algorithm described in the previous section.

The mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads.

The general algorithm works in the following manner. The source of the packet transmits the packet to its cluster-head. From this cluster-head, the packet is sent to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. The gateway sends it to that cluster-head and so on till the destination cluster-head is reached in this way. The destination cluster-head then transmits the packet to the destination. Figure 3 shows an example of CGSR routing scheme.
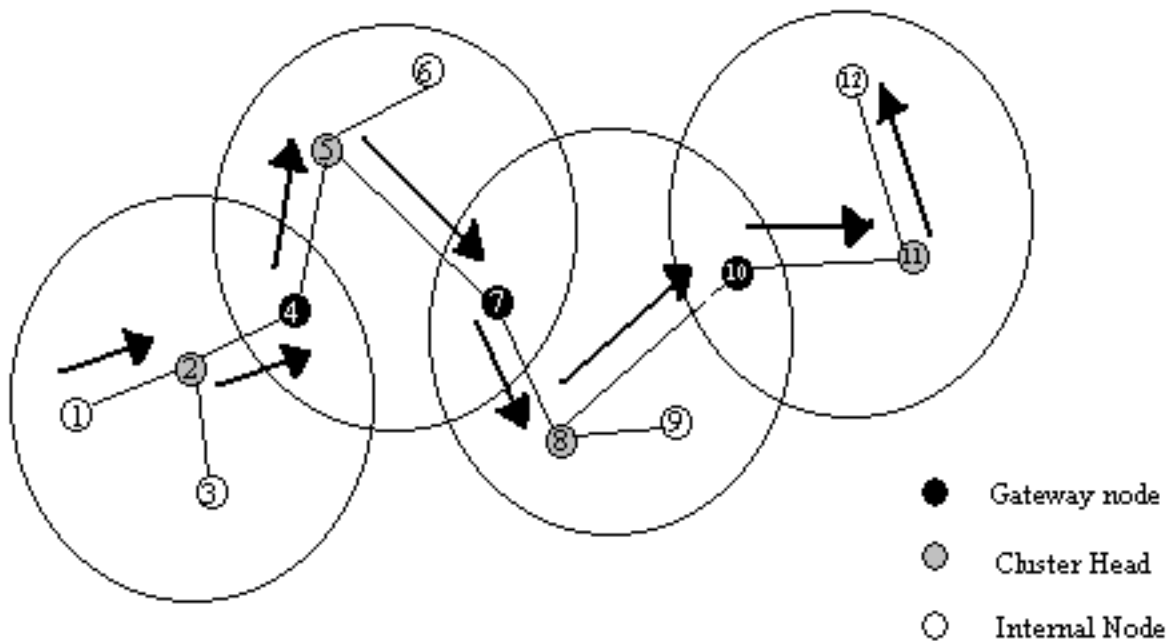
Figure 3. Example of CGSR routing from node 1 to node 12

Each node maintains a cluster member table that has mapping from each node to its respective cluster-head. Each node broadcasts its cluster member table periodically and updates its table after receiving other nodeÆs broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster.

On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

[Back to Table of Contents]

---

3. On-Demand Routing Protocols

These protocols take a lazy approach to routing. In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. This section discusses a few on-demand routing protocols.

3.1 Cluster based Routing Protocols

In Cluster Based Routing protocol (CBRP) [Jiang99], the nodes are divided into clusters. To form the cluster the following algorithm is used. When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a Hello message. When a cluster-head gets this hello message it responds with a triggered hello message immediately. When the undecided node gets this message it sets its state to

"member". If the undecided node times out, then it makes itself the cluster-head if it has bi-directional link to some neighbor otherwise it remains in undecided state and repeats the procedure again. Clusterheads are changed as infrequently as possible.

Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has entry that contains the gateway through which the cluster can be reached and the cluster-head of the cluster.

When a source has to send data to destination, it floods route request packets (but only to the neighboring cluster-heads). On receiving the request a cluster-head checks to see if the destination is in its cluster. If yes, then it sends the request directly to the destination else it sends it to all its adjacent cluster-heads. The cluster-heads address is recorded in the packet so a cluster-head discards a request packet that it has already seen. When the destination receives the request packet, it replies back with the route that had been recorded in the request packet. If the source does not receive a reply within a time period, it backs off exponentially before trying to send route request again.

In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. In local repair mechanism, when a node finds the next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

3.2 Ad hoc On-demand Distance Vector Routing

Ad hoc On-demand Distance Vector Routing (AODV) [Perkins99] is an improvement on the DSDV algorithm discussed in section 2.1. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 4a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 4b), the nodes along the path enter the forward route into their tables.

If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate

nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.
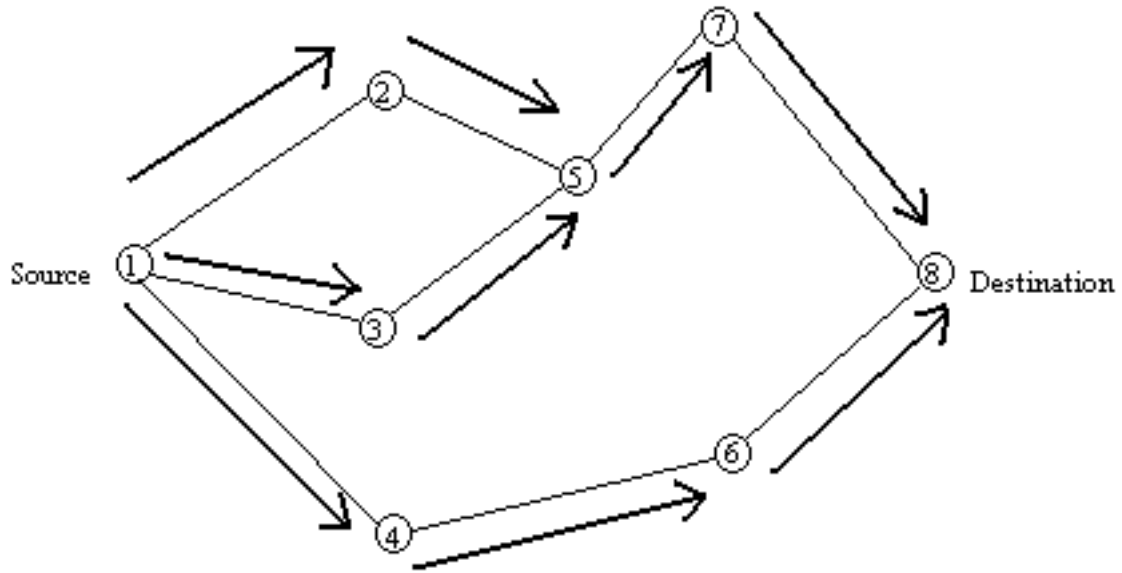
(a) Propogation of Route Request (RREQ) Packet
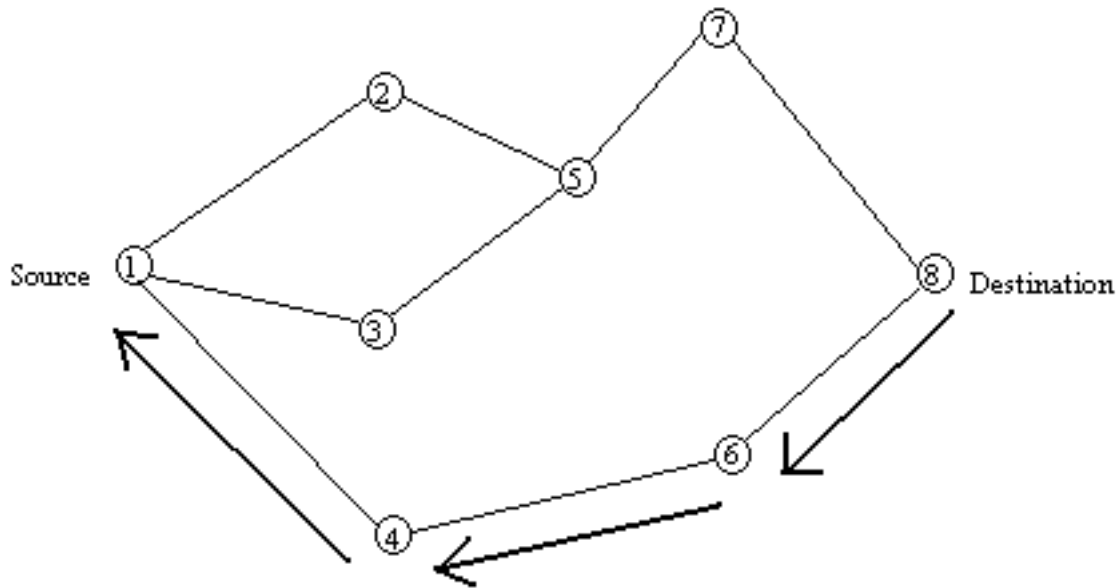
(b) Path taken by the Route Reply (RREP) Packet

Figure 4. Route discovery in AODV

3.3 Dynamic Source Routing Protocol

The Dynamic Source Routing Protocol [Johnson99] is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes.

The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet.

A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet [Johnson96]. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.
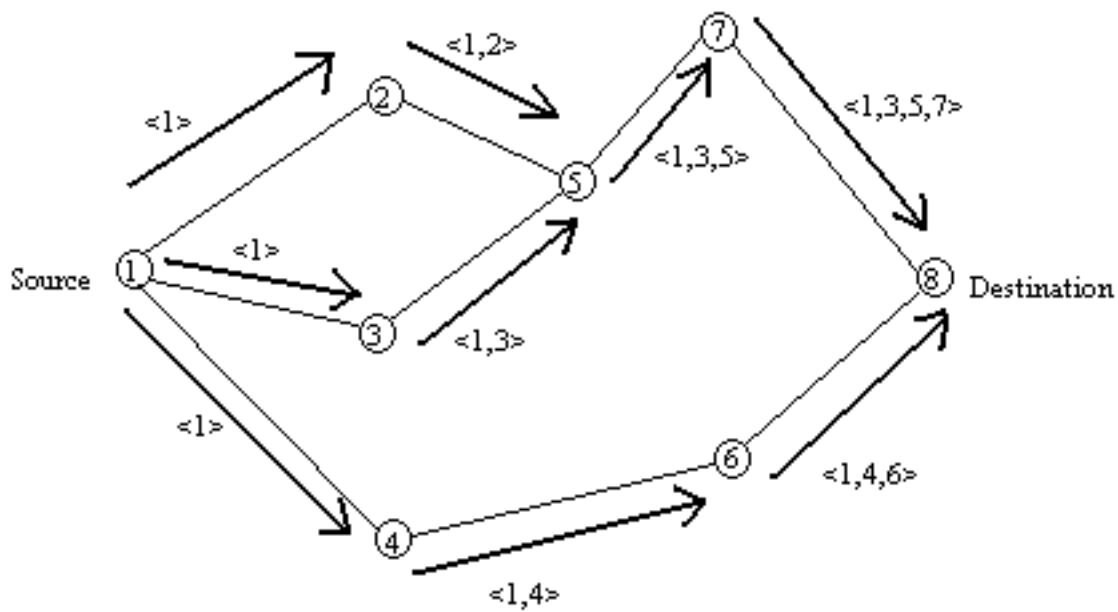
(a) Building Record Route during Route Discovery
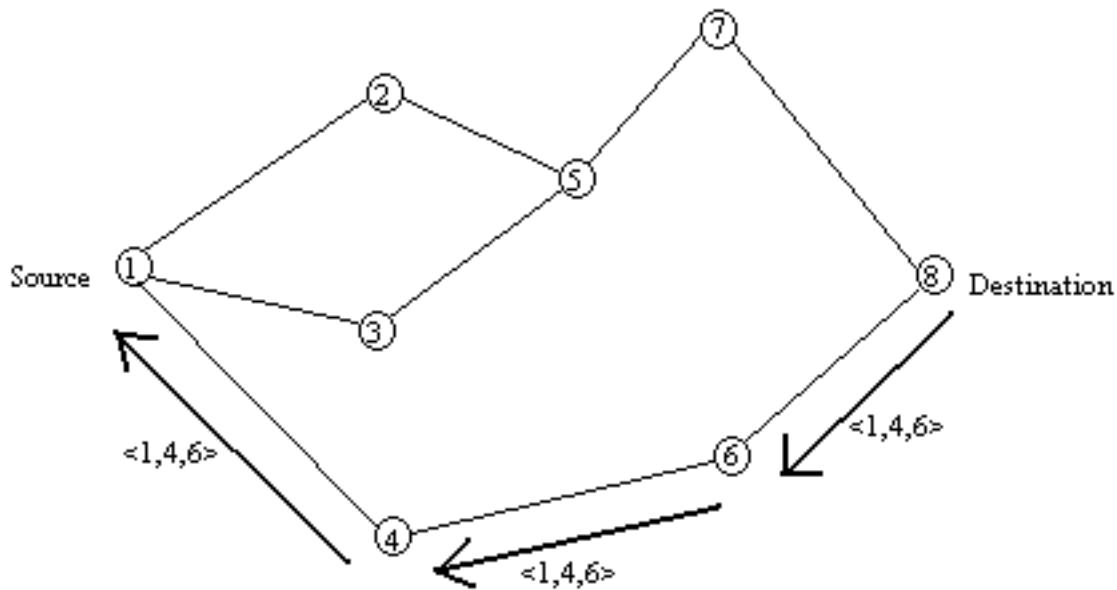
(b) Propogation of Route Reply with the Route Record

Figure 5. Creation of record route in DSRP

As the route request packet propagates through the network, the route record is formed as shown in figure 5a. If the route reply is generated by the destination then it places the route record from route request packet into the route reply packet. On the other hand, if the node generating the route reply is an intermediate node then it appends its cached route to destination to the route record of route request packet and puts that into the route reply packet. Figure 5b shows the route reply packet being sent by the destination itself. To send the route reply packet, the responding node must have a route to the source. If it has a route to the source in its route cache, it can use that route. The reverse of route record can be used

if symmetric links are supported. In case symmetric links are not supported, the node can initiate route discovery to source and piggyback the route reply on this new route request.

DSRP uses two types of packets for route maintenance:- Route Error packet and Acknowledgements. When a node encounters a fatal transmission problem at its data link layer, it generates a Route Error packet. When a node receives a route error packet, it removes the hop in error from it's route cache. All routes that contain the hop in error are are truncated at that point. Acknowledgment packets are used to verify the correct operation of the route links. This also includes passive acknowledgments in which a node hears the next hop forwarding the packet along the route.

# 3.4 Temporally Ordered Routing Algorithm

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal [Park97]. TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance, and Route erasure.

Each node has a quintuple associated with it -

- Logical time of a link failure
- The unique ID of the node that defined the new reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

The first three elements collectively represent the reference level. A new reference level is defined each time a node loses its last downstream link due to a link failure. The last two values define a delta with respect to the reference level [Park97].

Route Creation is done using QRY and UPD packets. The route creation algorithm starts with the height (propagation ordering parameter in the quintuple) of destination set to 0 and all other node's height set to NULL (i.e. undefined). The source broadcasts a QRY packet with the destination node's id in it. A node with a non-NULL height responds with a UPD packet that has its height in it. A node receiving a UPD packet sets its height to one more than that of the node that generated the UPD. A node with higher height is considered upstream and a node with lower height downstream. In this way a directed acyclic graph is constructed from source to the destination. Figure 6 illustrates a route creation process in TORA. As shown in figure 6a, node 5 does not propagate QRY from node 3 as it has already seen and propagated QRY message from node 2. In figure 6b, the source (i.e. node 1) may have received a UPD each from node 2 or node 3 but since node 4 gives it lesser height, it retains that height.
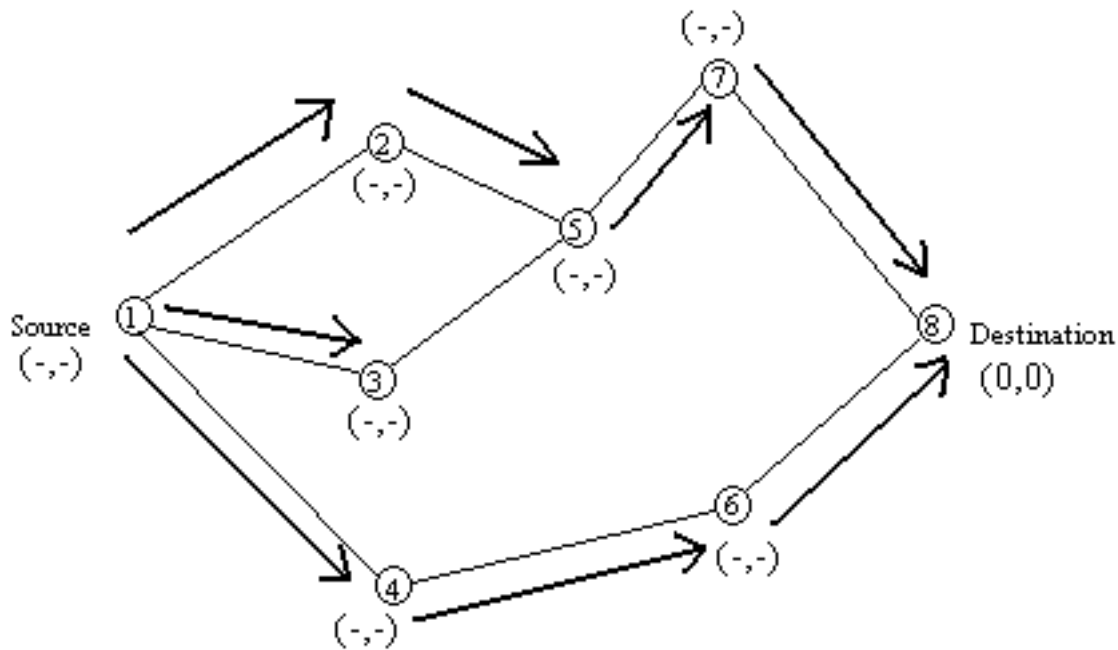
(a) Propogation of QRY message through the network
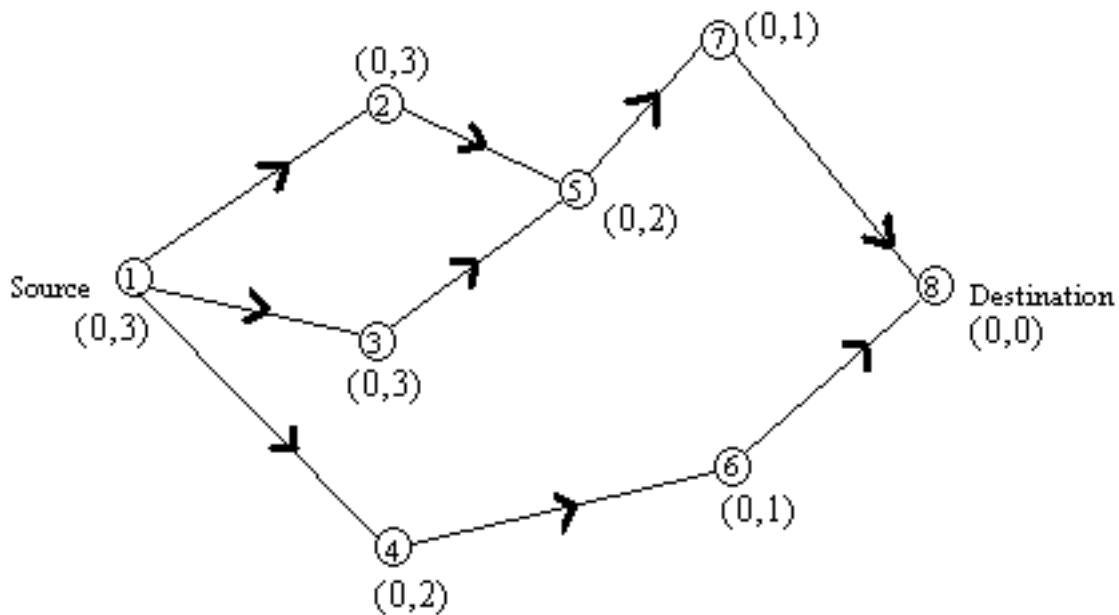
(b) Height of each node updated as a result of UPD messages

Figure 6. Route creation in TORA. (Numbers in braces are reference level, height of each node)

When a node moves the DAG route is broken, and route maintenance is needed to reestablish a DAG for the same destination. When the last downstream link of a node fails, it generates a new reference level. This results in the propagation of that reference level by neighboring nodes as shown in figure 7. Links are reversed to reflect the change in adapting to the new reference level. This has the same effect as reversing the direction of one or more links when a node has no downstream links.
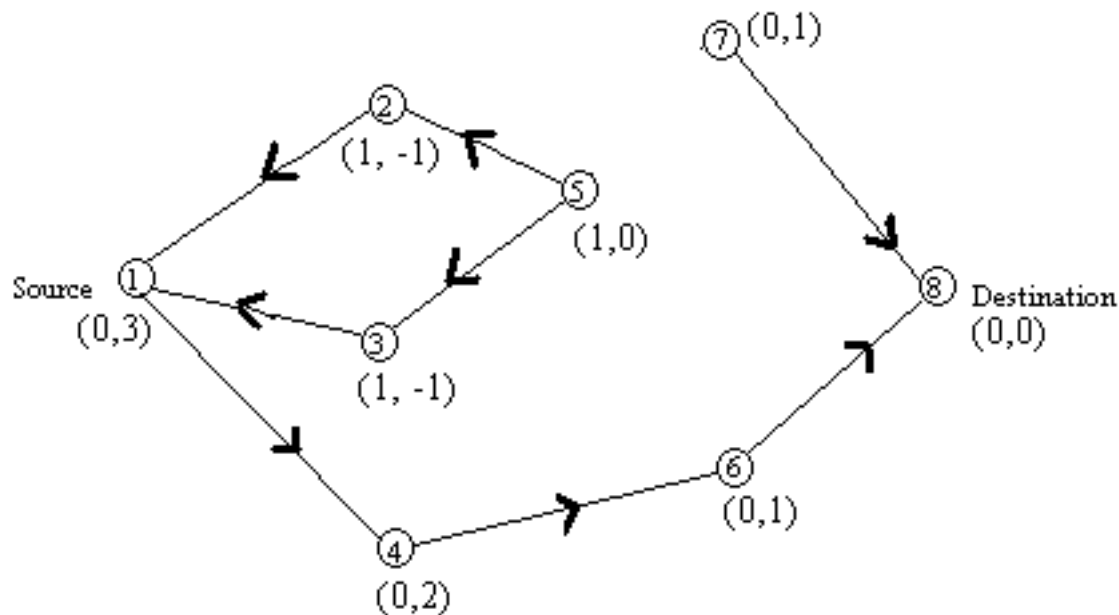
Figure 6. Re-establishing route on failure of link 5-7. The new reference level is node 5.

In the route erasure phase, TORA floods a broadcast clear packet (CLR) throughout the network to erase invalid routes.

In TORA there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Because TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will ultimately occur.

3.5 Associativity Based Routing

The Associativity Based Routing (ABR) protocol is a new approach for routing proposed in [Toh96,Toh99]. ABR defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be long-lived. All node generate periodic beacons to signify its existence. When a neighbor node receives a beacon, it updates its associativity tables. For every beacon received, a node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are Route discovery, Route reconstruction (RRC) and Route deletion.

The route discovery phase is a broadcast query and await-reply (BQ-REPLY) cycle. The source node broadcasts a BQ message in search of nodes that have a route to the destination. A node does not forward

a BQ request more than once. On receiving a BQ message, an intermediate node appends its address and its associativity ticks to the query packet. The next succeeding node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. Each packet arriving at the destination will contain the associativity ticks of the nodes along the route from source to the destination. The destination can now select the best route by examining the associativity ticks along each of the paths. If multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. Once a path has been chosen, the destination sends a REPLY packet back to the source along this path. The nodes on the path that the REPLY packet follows mark their routes as valid. All other routes remain inactive, thus avoiding the chance of duplicate packets arriving at the destination.

RRC phase consists of partial route discovery, invalid route erasure, valid route updates, and new route discovery, depending on which node(s) along the route move. Source node movement results in a new BQ-REPLY process because the routing protocol is source-initiated. The route notification (RN) message is used to erase the route entries associated with downstream nodes. When the destination moves, the destination's immediate upstream node erases its route. A localized query (LQ [H]) process, where H refers to the hop count from the upstream node to the destination, is initiated to determine if the node is still reachable. If the destination receives the LQ packet, it selects the best partial route and REPLYs; otherwise, the initiating node times out and backtracks to the next upstream node. An RN message is sent to the next upstream node to erase the invalid route and inform this node that it should invoke the LQ [H] process. If this process results in backtracking more than halfway to the source, the LQ process is discontinued and the source initiates a new BQ process.

When a discovered route is no longer needed, the source node initiates a route delete (RD) broadcast. All nodes along the route delete the route entry from their routing tables. The RD message is propagated by a full broadcast, as opposed to a directed broadcast, because the source node may not be aware of any route node changes that occurred during RRCs.

3.6 Signal Stability Routing

Signal Stability-Based Adaptive Routing protocol (SSR) presented in [Dube97] is an on-demand routing protocol that selects routes based on the signal strength between nodes and a node's location stability. This route selection criterion has the effect of choosing routes that have "stronger" connectivity. SSR comprises of two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

The DRP maintains the Signal Stability Table (SST) and Routing Table (RT). The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either recorded as a strong or weak channel. All transmissions are received by DRP and processed. After updating the appropriate table entries, the DRP passes the packet to the SRP.

The SRP passes the packet up the stack if it is the intended receiver. If not, it looks up the destination in the RT and forwards the packet. If there is no entry for the destination in the RT, it initiates a route-search process to find a route. Route-request packets are forwarded to the next hop only if they are received over strong channels and have not been previously processed (to avoid looping). The destination chooses the first arriving route-search packet to send back as it is highly likely that the packet arrived

over the shortest and/or least congested path. The DRP reverses the selected route and sends a route-reply message back to the initiator of route-request. The DRP of the nodes along the path update their RTs accordingly.

Route-search packets arriving at the destination have necessarily arrived on the path of strongest signal stability because the packets arriving over a weak channel are dropped at intermediate nodes. If the source times out before receiving a reply then it changes the PREF field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated.

When a link failure is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then sends an erase message to notify all nodes of the broken link and initiates a new route-search process to find a new path to the destination.

[Back to Table of Contents]

---

4. Conclusion

In this article, several existing routing protocols for ad hoc Wireless Networks were described. Two categories of routing protocols were discussed. Table-driven and on-demand routing protocols. In table-driven protocols, each node maintain up-to-date routing information to all the nodes in the network where in on-demand protocols a node finds the route to a destination when it desires to send packets to the destination.

Several table-driven protocols were discussed. DSDV and GSR are table-driven protocols that use destination sequence numbers to keep routes loop-free and up-to-date. HSR and ZHLS are hierarchical routing. FSR reduces the size of tables to be exchanged by maintaining less accurate information about nodes farther away. CGSR is a cluster-based routing protocol where nodes are grouped into clusters.

On-demand routing protocols were also discussed. In on-demand protocols, a route creation is initiated by the source when the source wants to communicate to the destination. CBRP is a cluster based routing algorithm like CGSR except that it is an on-demand routing mechanism as opposed to CGSR that is table-driven. AODV on-demand version of DSDV routing protocol. DSRP is a source routing mechanism where the route is in each packet. ABR uses the degree of associativity to select routes. Similarly, SSR selects routes based on signal strength.

[Back to Table of Contents]

---

5. References

- **[Royer99]** Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55, April 1999. http://users.ece.gatech.edu/~cktoh/royer.html

  Gives a review of routing protocols for ad hoc networks.

- **[Perkins94]** C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Comp. Comm. Rev., Oct. 1994, pp.234-244. http://www.svrloc.org/~charliep/txt/sigcomm94/paper.ps

  Discusses Destination-Sequenced Distance-Vector Routing Algorithm.

- **[Chiang97]** C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" Proc. IEEE SICON'97, Apr.1997, pp.197-211. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf

  Discusses Clustered Gateway Switch Routing Algorithm.

- **[Murthy96]** S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97. http://www.ics.uci.edu/~atm/adhoc/paper-collection/aceves-routing-winet.pdf

  Discusses Wireless Routing Protocol.

- **[Chen98]** Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC'98, 5 pages. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-gsr-icc98.pdf

  Discusses Global State Routing Algorithm.

- **[Iwata99]** A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79. http://www.cs.ucla.edu/NRL/wireless/PAPER/jsac99.ps.gz

  Discusses Fisheye State Routing and Hierarchical State Routing Algorithms.

- **[Joa-Ng99]** M Joa-Ng and I.-T. Lu, "A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1415-25.
  Discusses Zone-based Hierarchical Link State Routing Protocol.

- **[Jiang99]** Mingliang Jiang, Jinyang Li, Y.C. Tay, "Cluster Based Routing Protocol" August 1999 IETF Draft, 27 pages. http://www.ietf.org/internet-drafts/draft-ietf-manet-cbrp-spec-01.txt
  Discusses Cluster Based Routing Protocol.

- **[Perkins99]** Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, "Ad Hoc On-demand Distance Vector Routing", October 99 IETF Draft, 33 pages. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-04.txt
  Discusses Ad Hoc On-demand Distance Vector Routing Algorithm.

- **[Johnson96]** David B. Johnson, Davis A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer, 1996, pp. 152-81.

http://www.ics.uci.edu/~atm/adhoc/paper-collection/johnson-dsr.pdf
Discusses Dynamic Source Routing Algorithm.

- **[Johnson99]** David B. Johnson, Davis A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks" October 1999 IETF Draft, 49 pages.
  http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-03.txt
  Discusses Dynamic Source Routing Algorithm.

- **[Park97]** VD Park and MS Corson "A highly adaptive distributed routing algorithm for mobile wireless networks", Proc. INFOCOM'97, Apr. 1997, 9 pages.
  http://www.ics.uci.edu/~atm/adhoc/paper-collection/corson-adaptive-routing-infocom97.pdf
  Discusses Temporally Ordered Routing Algorithm.

- **[Toh96]** Chai-Keong Toh, "A novel distributed routing protocol to support Ad hoc mobile computing" Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480-86.
  http://www.ics.uci.edu/~atm/adhoc/paper-collection/toh-distributed-routing-ipccc96.pdf
  Discusses Associativity Based Routing Algorithm.

- **[Toh99]** C.-K. Toh, "Long-lived Ad-Hoc Routing based on the concept of Associativity" March 1999 IETF Draft, 8 pages.
  http://www.ietf.org/internet-drafts/draft-ietf-manet-longlived-adhoc-routing-00.txt
  Discusses Associativity Based Routing Algorithm.

- **[Dube97]** R. Dube et al., "Signal Stability based adaptive routing for Ad Hoc Mobile networks", IEEE Pers. Comm., Feb. 1997, pp. 36-45. http://www.cs.umd.edu/projects/mcml/papers/pcm97.ps
  Discusses Signal Stability Based Routing Algorithm.

- **[Haas98]** Z. J. Haas and M.R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM SIGCOMM'98.
  Describes ZRP protocol, which lead to the development of Zone-Based Hierarchical Routing Protocol.

[Back to Table of Contents]

List Of Acronyms:

DSDV - Dynamic Destination-Sequenced Distance-Vector Routing Protocol
WRP - The Wireless Routing Protocol
GSR - Global State Routing
FSR - Fisheye State Routing
HSR - Hierarchical State Routing
ZHLS - Zone-based Hierarchical Link State Routing Protocol
CGSR - Clusterhead Gateway Switch Routing Protocol
CBRP - Cluster based Routing Protocols
AODV - Ad Hoc On-demand Distance Vector Routing
DSRP - Dynamic Source Routing Protocol
TORA - Temporally Ordered Routing Algorithm

ABR - Associativity Based Routing
SSR - Signal Stability Routing

[Back to Table of Contents]

Date Last Modified: 11/18/99
Note: This paper is available on-line at
http://www.cis.ohio-state.edu/~jain/cis788-99/adhoc_routing/index.html