ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

A Survey on Routing Protocols in Wireless Ad HOC Networks

[I]K.S.Saravanan, [II]Dr. N.Rajendran
[I]Research Scholar, Bharathiar University, Coimbatore, India
[II]Principal, Vivekanandha Arts and Science College for Women, Sankari, India

Abstract
Wireless ad-hoc networks are perform many difficult jobs for communication in the environment of decentralized infrastructure such as mobile nodes, changing network topology, without base station and access points. The Wireless nodes are forming a short-term network without requirement of any existing infrastructure. In such an environment, to forward a packet from host to destination require a mobile host. In the last Twenty years, the wireless networking society has been designed hundreds of new routing protocols targeting the various design scenarios such as messages wants to delivered in a timely manner, bandwidth and power consumption, location of the nodes and so on. Routing protocols in ad-hoc networks specify communication between routers and enable them to select routes between a source and a destination. The choice of the routes is performed by routing algorithms. This article provides an overview of different ad hoc network protocols by presenting their functionality and discussion of their respective merits and drawbacks.

Key words
Ad HOC Networks, Routers, Routing Protocols

Introduction

Wireless Network Field has been growing extremely quick in last few of years. Wireless networks are classified in two types, infrastructure network and infrastructure less (ad hoc) networks. Infra-structured network are the network with fixed and wired gateways. Infrastructure mode wireless networking bridges a wireless network to a wired Ethernet network [1]. Infrastructure mode wireless also supports central connection points for WLAN clients. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other wireless ad hoc network devices in link range. Each ad hoc node may be capable of acting as a router. Such ad hoc networks may arise in personal area networking, meeting rooms and conferences, disaster relief and rescue operations, battlefield operations, etc. Ad hoc radio networks have various implementation areas. Some areas to be mentioned are military, emergency, conferencing and sensor applications. Each of these application areas has their specific requirements for routing protocols [2]. Ad hoc network is a multi-hop wireless network, which consists of number of mobile nodes. These nodes generate traffic to be forwarded to some other nodes or a group of nodes. Due to a dynamic nature of ad hoc networks, traditional fixed network routing protocols are not viable. Based on that reason several proposals for routing protocols have been presented [3]. This article examines routing protocols designed for these ad hoc networks by first describing the operation of each of the protocols, the next section presents a discussion of four subdivisions of ad hoc routing protocols. Another section discusses current table-driven protocols, while a later section describes those protocols which are classified as on-demand. The article then presents many ad hoc wireless networks routing protocols are discussed; and finally, the last section concludes the article.

Wireless Ad Hoc Routing Protocols

Since the advent of Defense Advanced Research Projects Agency (DARPA) packet radio networks in the early 1970s, numerous protocols have been developed for ad hoc wireless networks. Such protocols must deal with the typical limitations of these networks, which include high power consumption, low bandwidth, and high error rates.

These wireless ad hoc routing protocols can be classified into four categories, which are based on:

- Routing information update mechanism;
- Usage of temporal information (e.g. cached routes);
- Usage of topology information;
- Usage of specific resources (e.g. GPS).

Based on routing information update mechanism :

- Proactive (table-driven) routing protocols;
- Reactive (on-demand) routing protocols;
- Hybrid protocols.

Based on usage of temporal information

- Based on past temporal information;
- Based on future temporal information.

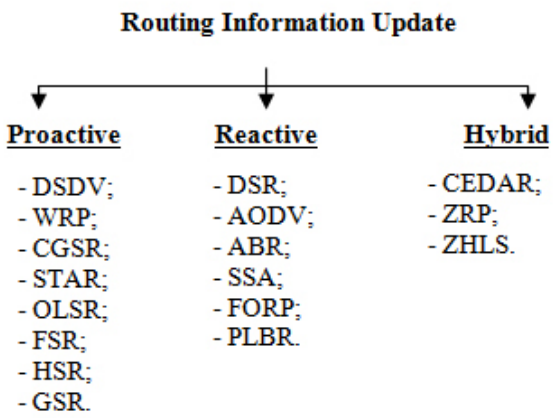
Based on the routing topology

- Flat topology routing protocols:
- Hierarchical topology routing protocols

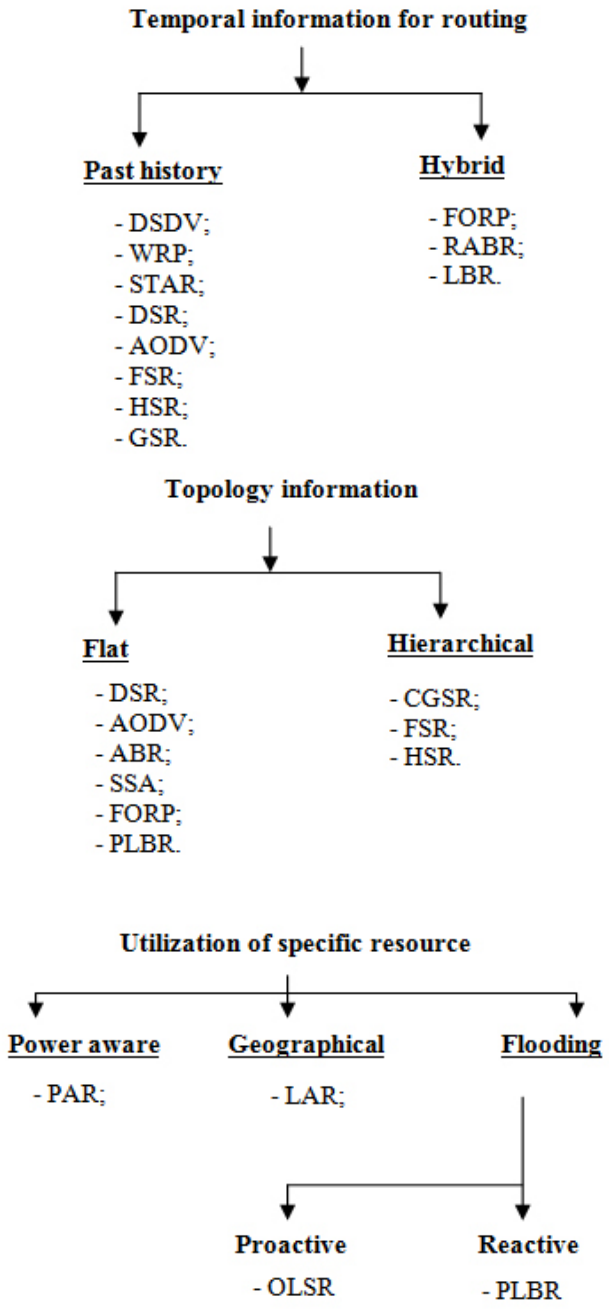
Routing based on utilization of specific resources:

- Power-aware routing;
- Geographical information assisted routing.

The analyze of these categories Routing Protocols are given below,



ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)



The discussions of routing protocols are given below,

Destination-Sequenced Distance-Vector Routing

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the table-driven algorithm and based on the classical Bellman-Ford Routing Algorithm with certain improvements[4][5]. Every wireless 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 shown in Figure1. 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 [6].

Dest	Next	Dist
6	3	2
5	3	2
4	2	2

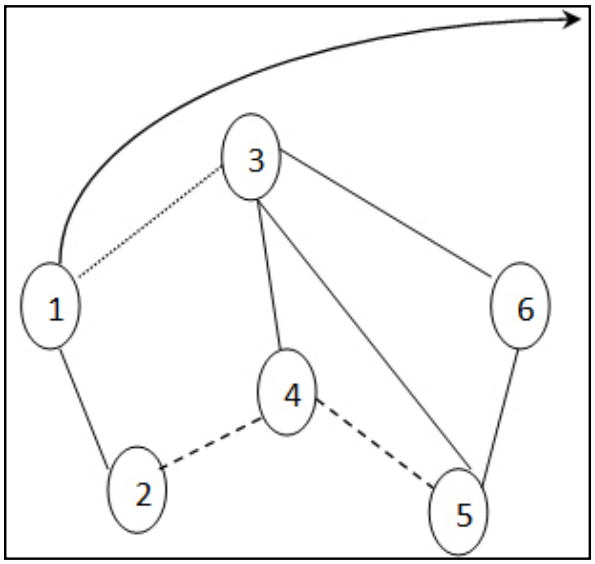


Fig. 1: DSDV Routing

The Wireless Routing Protocol (WRP)

This is a proactive, destination-based protocol and table-based distance-vector routing protocol. WRP belong to the class of path finding algorithms. Path-finding algorithms eliminate the counting-to-infinity problem of distributed Bellman- Ford-algorithms by using that predecessor information, which can be used to infer an implicit path to a destination and thus detect routing loops. In WRP there is a quite complicated table structure. Each node maintains four different tables as in many other table-driven protocols only two tables are needed.

These four tables are:

1) Distance table,
2) Routing table,
3) Link cost table
4) Message retransmission list (MRL) table.

I) 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.

II) 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.

III) 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.

IV) 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. 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. 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 [8].

Cluster head Gateway Switch Routing protocol (CGSR)

It is a multichannel operation capable protocol. It enables code separation among clusters. The clusters are formed by cluster head election procedure, which is quite intensive process. On that reason the protocol uses so called Least Cluster Change (LCC) algorithm for that election among two cluster heads. CGSR is not an autonomous protocol. It uses DSDV as the underlying routing scheme. The DSDV approach is modified to use a hierarchical cluster head-to-gateway routing. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, until the destination node's cluster head is reached. That destination cluster head then transmits the packet to the destination node. 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 2 shows an example of CGSR routing scheme.

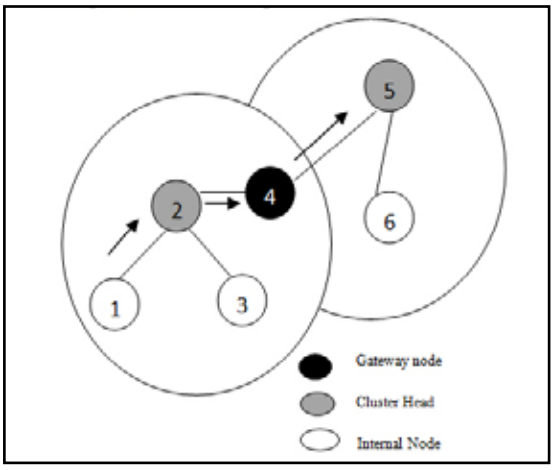


Fig. 2 : CGSR Routing scheme

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 node broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster [9,10].

Fisheye State Routing (FSR): 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 3 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 [11].

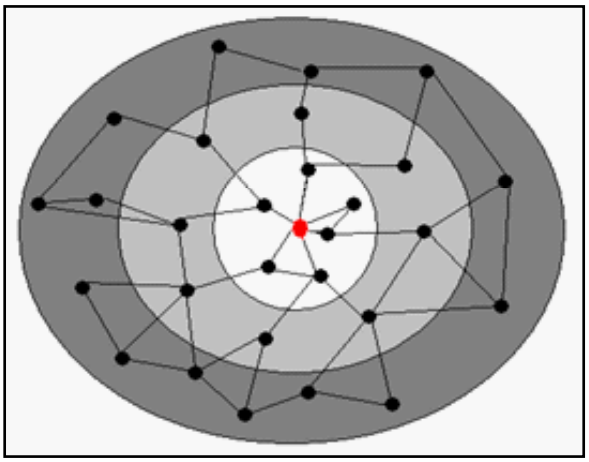


Fig. 3: Fisheye State Routing

Hierarchical State Routing (HSR)

It is a class of protocols based on multilevel clustering. The goal is to replace the flooding of the control information with a local collection of this information in the cluster head, followed by the propagation of this information to the other cluster heads. First, nodes form level 0 clusters based on physical proximity and elect a cluster head. Cluster heads connect to each other using virtual links. Multiple cluster heads can assemble themselves into higher level clusters. When a node changes its position, link state information is exchanged between cluster heads using the virtual links. The cluster head collects link state information about the nodes in its cluster and propagates it to other cluster heads through gateway nodes. Routing in HSR happens using a hierarchical addressing scheme, with the cluster head acting as routers. When a node wants to send a packet, it sends it first to the local cluster head. The cluster head looks up the destination and sends the packet to its nearest gateway node. The gateway node then propagates the packet to the nearest gateway node at the next level of the hierarchy. The process continues until the packet reaches the gateway node of the destination cluster. The final gateway node routes the packet to the cluster head of the destination cluster which then forwards

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the packet to the destination node [12].

Global State Routing (GSR)is a uniform, topology oriented, proactive routing protocol. 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. 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. Based on the complete topology information in the topology table, any shortest-path algorithm can be used to compute a routing table containing the optimal next - hop information for each destination. GSR defines a variant of Dijkstra's algorithm for this purpose [13].

Optimized Link State Routing (OLSR) is a topology based, neighbor selection protocol, in which each node only maintains a subset of network topology information. OLSR is a proactive protocol, because it exchanges the topology information with other nodes regularly to maintain information required for routing. OLSR reduces the cost of distributing network-scale link-state information by two ways. First, it uses multipoint relays (MRP) to reduce redundant rebroadcasting during flooding operation. That is the key concept of the protocol. MRPs are selected nodes, which forward broadcast messages during the flooding process. Secondly each node only broadcast the state of nodes in its own multi-point relay set. That is a method to reduce the contents of the control messages. A node's multipoint relay set is the minimal subset of its one-hop neighbors, which must rebroadcast a message so that it is received by all of its two-hop neighbors. When a node sends a broadcast message, all of its neighbors receive and process the data. However, only those neighbors, which belongs to the source node's MPR set and have not previously received the message re-broadcast it. This reduces the number of broadcast messages needed to flood a message through the network. Since each node selects its MPR set independently, it must know the topology of its two-hop neighborhood, but additional inter-nodal coordination is not required [14].

Dynamic Source Routing (DSR)

This protocol presented in [15] is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: Route discovery and Route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. Figure 4 illustrates the formation of the route record as the route request propagates through the network. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator.

Route maintenance is accomplished through the use of route error packets and acknowledgments. Route error packets are generated at a node when the data link layer encounters a fatal transmission problem. When a route error packet is received, the hop in error is removed from the node's route cache and all routes containing the hop are truncated at that point. In addition to route error messages, acknowledgments are used to verify the correct operation of the route links. Such acknowledgments include passive acknowledgments, where a mobile is able to hear the next hop forwarding the packet along the route.

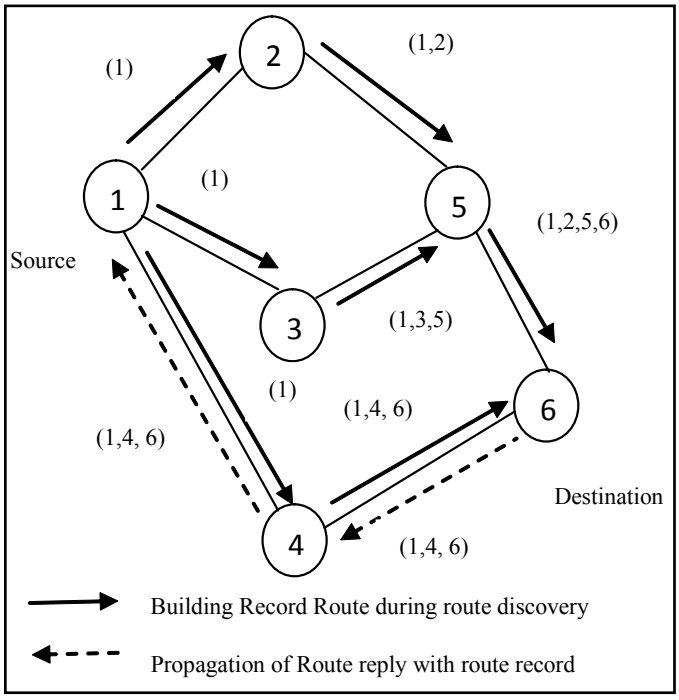


Fig. 4 : DSR Routing Record and Reply

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 its route cache. All routes that contain the hop in error 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.

Ad Hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in [16] builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. Figure 3a illustrates the propagation of the broadcast RREQs across the network. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by uncasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ (Figure 5). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message (an RREP with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route [7]. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired.

An additional aspect of the protocol is the use of hello messages, periodic local broadcasts by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node. However, the use of hello messages is not required. Nodes listen for retransmission of data packets to ensure that the next hop is still within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages, to determine whether the next hop is within communication range. The hello messages may list the other nodes from which a mobile has heard, thereby yielding greater knowledge of network connectivity.

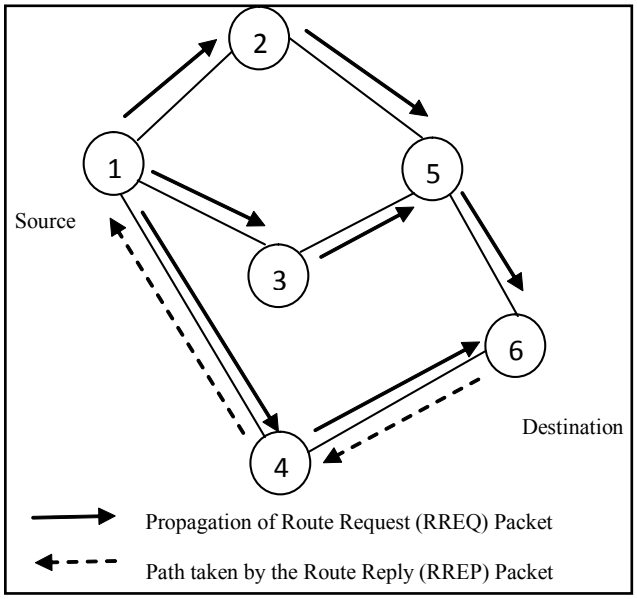


Fig. 5 : AODV Routing Request and Reply

Associatively-Based Routing — A totally different approach in mobile routing is proposed in [17]. The Associatively- Based Routing (ABR) protocol is free from loops, deadlock, and packet duplicates, and defines a new routing metric for ad hoc mobile networks. This metric is known as the degree of association stability. Association stability is defined by connection stability of one node with respect to another node over time and space. A high degree of association stability may indicate a low state of node mobility, while a low degree may indicate a high state of node mobility. Associatively ticks are reset when the neighbors of a node or the node itself move out of proximity. A fundamental objective of ABR is to derive longer-lived routes for ad hoc mobile networks.

The three phases of ABR are:

- Route discovery
- Route reconstruction (RRC)
- Route deletion

The route discovery phase is accomplished by a broadcast query and await-reply (BQ-REPLY) cycle. A node desiring a route broadcasts a BQ message in search of mobiles that have a route to the destination. All nodes receiving the query (that are not the destination) append their addresses and their associatively ticks with their neighbors along with QoS information to the query packet. A successor node erases its upstream node neighbors' associatively tick entries and retains only the entry concerned with itself and its upstream node. In this way, each resultant packet arriving at the destination will contain the associatively ticks of the nodes along the route to the destination. The destination is then able to select the best route by examining the associatively ticks along each of the paths. When multiple paths have the same

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

overall degree of association stability, the route with the minimum number of hops is selected. The destination then sends a REPLY packet back to the source along this path. Nodes propagating the REPLY mark their routes as valid. All other routes remain inactive, and the possibility of duplicate packets arriving at the destination is avoided. RRC may consist of partial route discovery, invalid route ,erasure, valid route updates, and new route discovery, depending on which node(s) along the route move. Movement by the source results in a new BQ-REPLY process, as shown in Fig.6a. The RN[1] message is a route notification used to erase the route entries associated with downstream nodes. When the destination moves, the immediate upstream node erases its route and determines if the node is still reachable by a localized query (LQ[H]) process, where H refers to the hop count from the upstream node to the destination (Figure 6a and 6b). If the destination receives the LQ packet, it REPLYs with the best partial route; otherwise, the initiating node times out and the process backtracks to the next upstream node. Here an RN[0] 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 a new BQ process is initiated at the source.

When a discovered route is no longer desired, the source node initiates a route delete (RD) broadcast so that all nodes along the route update 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.

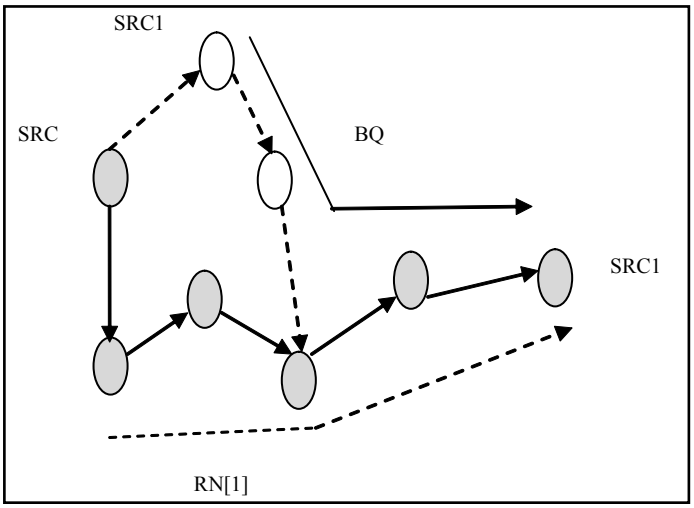


Fig. 6a : Route of source Move

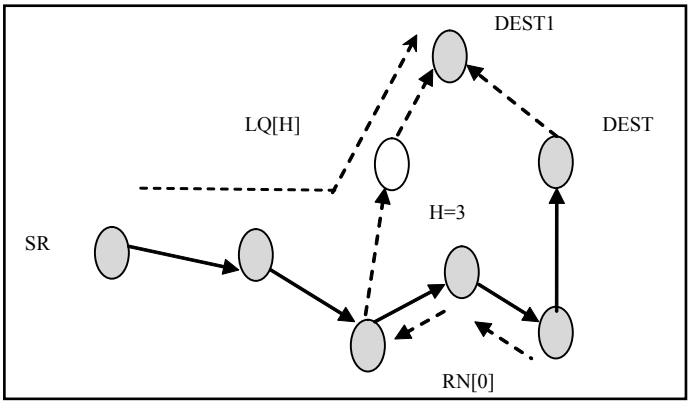


Fig. 6b: Route of Destination Move

Signal Stability Routing — Another on-demand protocol is the Signal Stability-Based Adaptive Routing protocol (SSR) presented in [18]. Unlike the algorithms described so far, SSR selects routes based on the signal strength between nodes and a node's location stability. This route selection criteria has the effect of choosing routes that have "stronger" connectivity. SSR can be divided into two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP).

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

The SRP processes packets by passing the packet up the stack if it is the intended receiver or looking up the destination in the RT and then forwarding the packet if it is not. If no entry is found in the RT for the destination, a route-search process is initiated to find a route. Route requests are propagated throughout the network, but are only forwarded to the next hop if they are received over strong channels and have not been previously processed (to prevent looping). The destination chooses the first arriving route-search packet to send back because it is most probable that the packet arrived over the shortest and/or least congested path. The DRP then reverses the selected route and sends a route-reply message back to the initiator. The DRP of the nodes along the path update their RTs accordingly. Route-search packets arriving at the destination have necessarily chosen the path of strongest signal stability, since the packets are dropped at a node if they have arrived over a weak channel. If there is no route-reply message received at the source within a specific timeout period, the source 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 failed link is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then initiates another route-search process to find a new path to the destination. The source also sends an erase message to notify all nodes of the broken link.

The Flow Oriented Routing Protocol (FORP) [19]

The FORP protocol proposed by Su and Gerla aims to transmit real-time data streams in ad hoc networks, which require in-order delivery of packets with tight delivery bounds. If alternate routes are not available to immediately redirect the data packets in case of route failures, real-time packets may be dropped. FORP introduces the "multi-hop handoff" mechanism in which the nodes use their mobility information to determine future route changes resulting in rebuilding of an alternate route much sooner.

Similarly to other on-demand schemes, FORP maintains routing information only for active source/destination pairs. The protocol predicts the link expiration time (LET) for each hop on the route to calculate the route expiration time (RET). During the route discovery phase, the source broadcasts a Flow-REQ message containing a sequence number, source ID, and destination ID. Each node appends its own ID and the LET of the last link in which the message was received before forwarding to the next hop. When the Flow-REQ arrives at the destination, it contains the list of all the routes travelled and the LETs for each hop. Using this information, the destination calculates the RET by selecting

the minimum LET value for the route. The nodes are assumed to have a common time reference from GPS for instance. Once the route is selected, a Flow-SETUP message travels to the source along the chosen path.

While the connection is in progress, the intermediate nodes continue adding the LETs to the forwarded packets to enable the destination to keep track of the RET prediction. If the destination determines that a "critical time" is reached, i.e. the route is close to expire, a Flow-HANDOFF message is generated and propagated throughout the network. These Flow-HANDOFF messages reach the source and based on their LETs and RET, the source determines the new route. The "critical time" is calculated as Tc = RET - Td where RET is the route expiration time and Td is the delay experienced by the last packet arrived on the same route.

Core-Extraction Distributed Ad Hoc Routing (CEDAR) [20]

The CEDAR protocol, proposed by Sivakumar et al. is allows the consideration of QoS requirements in an ad hoc setting. The protocol selects a subset of nodes called the core of the network. Control messages will only be broadcasted among the nodes of the core, which can use any existing ad hoc routing mechanism for communication. The core is positioned as a "self-organizing routing infrastructure" which performs route availability computations through waves of messages with dynamically limited propagation speed. The availability of increased bandwidth is transmitted by slow propagating increase waves, while information about decreased bandwidth is transmitted by fast propagating decrease waves.

Routing in the CEDAR architecture happens as follows. The source node sends a route request packet containing the source, destination, and the requested bandwidth to its dominator, the local core node. The dominator then computes and establishes a QoS route if feasible. The dominator nodes in each cluster maintain local state information and communicate with each other using virtual links. Route computation is carried out only on the core path. CEDAR aims more at robustness than optimality in computing the routes. Each core node only knows about the neighboring core node and has no global knowledge about the core subgraph. This simplifies the maintenance of the core network which can be necessary due to topology changes induced by the mobility or failure of nodes. Core paths are established on-demand for connection requests and route computation is carried out only when a specific request for a route is received.

Zone Routing Protocol (ZRP) [21]

The ZRP protocol, designed by Samar et al. is designed to be used in large scale networks. The protocol uses a pro-active mechanism of node discovery within a node's immediate neighborhood while inter-zone communication is carried out by using reactive approaches. Local neighborhoods, called zones, are defined for nodes (see Figure 16). The size of a zone is based on factor defined as the number of hops to the perimeter of the zone. There may be various overlapping zones which help in route optimization.

Neighbor discovery is accomplished by either Intrazone Routing Protocol (IARP) or simple Hello packets. IARP is pro-active approach and always maintains up-to-date routing tables. Since the scope of IARP is restricted within a zone, it is also referred to as "limited scope pro-active routing protocol". Route queries outside the zone are propagated by the route requests based on the perimeter of the zone (i.e. those with hop counts equal to ρ), instead of flooding the network. The Interzone Routing Protocol (IERP) uses a reactive approach for communicating with nodes in different zones. Route queries are forwarded to peripheral nodes using the border cast resolution protocol (BRP). The ZRP architecture can be seen in Figure 17.

Zone based Hierarchical Link State routing protocol (ZHLS) [22]

Joa-Ng and Lu propose ZHLS routing protocol where a hierarchical structure is defined by non-overlapping zones with each node having a node ID and a zone ID. These IDs are calculated using an external location tool such as GPS. The hierarchy is divided into two levels: the node level topology and the zone level topology. There are no Cluster heads in ZHLS. When a route is required for a destination located in another zone, the source node broadcasts a zone-level location request to all other zones. Once the destination receives the location request, it replies with the path. In this technique, only the node and zone IDs of a node is required to discover a path. There is no need for updates as long as the node stays within its own region and the location update is required only if the node switches regions. The only drawback of ZHLS is that all nodes should have a preprogrammed static zone map to recognize the zones created in the network. This may not be possible in scenarios where the network boundaries are dynamic in nature. On the other hand, it is suitable for the networks deployed with fixed boundary lines.

Source-Tree Adaptive Routing (STAR) [23]

Garcia-Luna-Aceves and Spohn propose STAR where each node maintains a source tree which contains preferred links to all possible destinations. Nearby source trees exchange information to maintain up-to-date tables. A route selection algorithm is executed based on the propagated topology information to the neighbors. The routes are maintained in a routing table containing entries for the destination node and the next hop neighbor. The link state update messages are used to update changes of the routes in the source trees. Since these packets do not time out, no periodic messages are required. The STAR protocol provides two distinct approaches: optimum routing (ORA) and least overhead routing (LORA). The ORA approach obtains the shortest path to the destination while LORA minimizes the packet overhead. STAR also requires a neighbor protocol to make sure that each node is aware of its active neighbors. The STAR protocol has been further developed as SOAR.

Conclusion

In this article we discuss about several routing protocols for ad hoc wireless networks. We also provide a classification of these protocols according to the routing techniques. The main difference between the protocols is the ways of finding and maintaining the routes between source-destination pairs. The field of ad hoc mobile networks is rapidly growing and changing, and while there are still many challenges that need to be met, it is likely that such networks will see widespread use within the next few years.

Reference

[1] *N. Asokan and P. Ginzboorg. Key agreement in ad-hoc networks. Computer Communication Review, 23(17):1627–1637, Nov. 2000.*

[2] *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*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the Fourth Annual International Conference on Mobile Computing and Networking, pages 85–97, 1998.

[4] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Comp. Commun. Rev., Oct. 1994, pp. 234–44.

[5] L. R. Ford Jr. and D. R. Fulkerson, Flows in Networks, Princeton Univ. Press, 1962.

[6] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM, pages 234–244, August-September 1994.

[7] S. Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. MONET, 1(2):183–197,1996.

[8] 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.

[9] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. IEEE SICON '97, Apr. 1997, pp. 197–211.

[10] W. L. C. Chiang, H. Wu and M. Gerla. Routing in clustered multihop, mobile wireless networks. In Proceedings of IEEE SICON, pages 197–211, April 1997.

[11] 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.

[12] P. Krishna, M. Chatterjee, N. Vaidya, and D. Pradhan. A cluster-based approach for routing in ad hoc networks. In USENIX Symposium on Location Independent and Mobile Computing, April 1995.

[13] T. Chen, M. Gerla, "Global State Routing: A new Routing Scheme for Ad-Hoc Wireless Networks", Proceedings of IEEE ICC'98, pages 171-175, August 1998.http://www1.ics.uci.edu/~atm/adhoc/papercollection/ papers.html

[14] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. In Proceedings of IEEE INMIC, pages 62–68, December 2001.

[15] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, 1996, pp. 153–81

[16] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90–100.

[17] C-K. 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.

[18] R. Dube et al., "Signal Stability based Adaptive Routing (SSA) for Ad- Hoc Mobile Networks," IEEE Pers. Commun., Feb. 1997, pp. 36–45.

[19] W. Su and M. Gerla. IPv6 flow handoff in ad-hoc wireless networks using mobility prediction. In Proceedings of IEEE GLOBECOM, pages 271–275, December 1999.

[20] R. Sivakumar, P. Sinha, and V. Bharghavan. CEDAR: a core-extraction distributed ad hoc routing algorithm. IEEE Journal on Selected Areas in Communications, 17(8):1454–1465, 1999.

[21] P. Samar, M. Pearlman, and S. Haas. Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks. IEEE/ACM Transactions on Networking, 12(4):595–608, August 2004.

[22] M. Joa-Ng and I.-T. Lu. A peer-to-peer zone-based two-level link state routing for mobile ad hoc network. IEEE Journal on Selected Areas in Communications, 17(8):1415–1425, 1999.

[23] J. J. Garcia-Luna-Aceves and M. Spohn. Source-tree routing in wireless networks. In Proceedings of IEEE ICNP, pages 273–282, October-November 1999.

Authors Profile

K.S.Saravanan received his M.Phil(C.S) Degree from Periyar University in the year 2008. He has received his M.C.A, Degree from Bharathiar University, Coimbatore in the year 2000. He is working as Assistant Professor, Department of Computer Application, Vivekanandha College of Arts and Science for Women, Namakkal, Tamilnadu, India. His areas of interest include Networking and Wireless Sensor Networks. Networks.

Dr. N.Rajendran received his Ph.D Degree from Periyar University, Salem in the year 2011. He has received his M.Phil, Degree from Bharathiar University, Coimbatore in the year 2000. He has received his M.C.A Degree from Madras University, Chennai in the year 1990. He is working as Principal of Vivekanandha Arts and Science College for Women, Sankari, Salem , Tamilnadu, He has 23 years of experience in academic field. He has published 06 International Journal papers and 13 papers in National and International Conferences. His areas of interest include Digital Image Processing and Networking.