Vandana Publications
IJEMR

Volume-4, Issue-1, February-2014, ISSN No.: 2250-0758

International Journal of Engineering and Management Research

Available at: www.ijemr.net

Page Number: 249-257

A Characteristics Study of Routing Protocols for Ad Hoc Wireless Networks

Alka Gupta[1], Dr. Sohan Garg[2]
[1]Research Scholar, INDIA
[2]SCRIET- CCS University Campus Meerut, INDIA

I. ABSTRACT & INTRODUCTION

Ad hoc networks are wireless mobile networks that do not rely on preexisting infrastructure and these networks allow a more flexible model of communication than traditional networks since the user is not limited to a fixed physical location. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route Ad hoc networks consist of mobile nodes equipped with wireless radio. If two such nodes are in mutual transmission range of each other then they can communicate directly. But if we want to forward the data from a source node to a destination node and these nodes are not within the transmission range of each other then a route from source to destination node is routed by intermediate nodes or we can say that intermediate nodes do routing in ad hoc wireless network. These intermediate nodes are called the routers. So the central task of a router is to forward packets from source node to a destination node, but in mobile ad hoc network (MANET} there are no predefined nodes acting as routers. Each node in the network can be used as a packet forward router; it means that there is no default router available in ad hoc wireless network.

PDA (Personal Digital Assistant) is primarily a business phone. Another word for a PDA: Handheld or Palmtop. A PDA is mainly aimed at business functions. A smart phone is a cell phone supported with advance features like 3G, GPRS, Wi-Fi, camera, speaker phone, and organizer, unlike PDA phones which are high end organizer phone. QWERTY keypads, and touch screen are a must for data entry on PDA phones irrespective of smart phone which work well with normal number pad alone. To enhance the life and performance of these phones it is advisable to have some necessary accessories like safety pouches, memory cards, Bluetooth head sets, screen protectors and portable key boards.PDA stands for construction should be done with a minimum of overhead and bandwidth consumption. In this paper, we present routing protocols designed for these ad hoc networks by describing the operation of each of the protocols. The remainder of the paper is organized as follows. The next section presents a discussion of two 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 paper then presents qualitative comparisons of table-driven protocols, followed by demand-driven and on-demand protocols; and finally, the last section concludes the paper.

Personal Digital Assistant and is primarily a business phone.

Simply, routing [10] is to make a decision for forwarding a packet from source to destination & the need of routing can be clear with the help of following example. In the case where only two hosts, within the transmission range, are involved in the ad hoc network, no real routing protocol or routing decisions are necessary. But in many practical ad hoc networks, two hosts that wish to correspond may not close enough to be within wireless transmission range of each other. These hosts could communicate if other hosts between them also participating in the ad hoc network are willing to forward packets for them.

As an example, consider the figure shown below. Mobile host *C* is not within the range of host *A*'s wireless transmitter (indicated by the circle around *A*) and host *A* is not within the range of host *C*'s wireless transmitter. Now, if *A* and *C* wish to interact with each other, they may in this case procure the services of host *B* to forward packets for them, since host *B* lies within the transmission range of both *A* and *C*. However middle node B can be used to forward packets between outermost nodes. The middle node B is

Acting as a router & this type of technique is known as a routing technique.

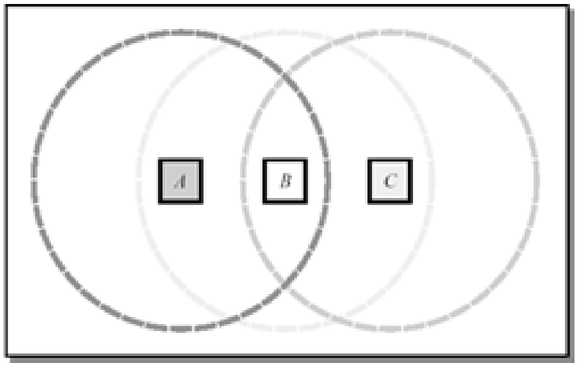


Figure 2.1 Example of Routing Techniques.

If node A is able to establish direct communication with node B in above figure, verified by exchanging suitable control messages between them, they both update their routing tables. When a third node C joins the network with the beacon signal, two scenarios are possible. The first is where both A and B establish that single-hop communication with C is possible. The second is where only one of the nodes, say B, recognizes the beacon signal from C and establishes the availability of direct communication with C. The distinct topology updates, consisting of both address and route updates, are made in all three nodes immediately afterward. In the first case, all routes are direct. In the other, the route update first happens between B and C, then between B and A, and then again between B and C, confirming the mutual reach ability relations to change in time, requiring route updates. Assume that for some reason the link between B and C are still reachable from each other, although this time only via node D and E .All five nodes in above figure are required to update their routing table appropriately to reflect this topology change, which will first be detected by nodes B and C, then communicated to A . As more nodes join the network or some of the existing nodes leave, the topology updates become more numerous, complex, and usually more frequent, thus diminishing the network resources available for exchanging user information.

However, in a real ad hoc network, the routing problem is much more complicated than the above example suggested, because of the complex network topology, no uniform propagation of wireless transmission and the movement of the intermediate nodes. Because of the fact that it may be necessary to hop several hops (multi hop) before a packet reaches the destination, a routing protocol/algorithm is needed. The routing protocol has two main functions, selection of routes for various sources – destination pairs and the delivery of messages to their correct destination. The second function is conceptually straightforward using a variety of protocols and data structures. This report is focused on selecting and finding routes.

II. LINK STATE ROUTING

Link state routing [67], each router has a complete picture of the whole network topology. Each router checks the cost of the link to each of its neighbor routers, and floods periodically updated information to all other routers in the network. After each router receives this updated information of the cost of each link in the network, each router calculates the shortest path to each possible destination. When each router needs to forward a packet to some destination, it transmits the packet to the next hop router based on the best path to the destination acquired from the updated information. The link state routing protocols show high speed of convergence to the correct network picture when the network is changed. However, in general, compared to the distance vector algorithm, this protocol requires more CPU time for computing the complete shortest route to each possible destination, and more network bandwidth for broadcasting the routing updates from each router to all other routers in the whole network. In order to reduce the disadvantage of the link state routing algorithm, one optimized protocol is proposed, called an Optimized Link State Routing (OLSR) [13].

OLSR is one of protocols using link state routing with a proactive nature, which allows periodic exchange of knowledge of network topology among all the nodes of the network. Because of this proactive nature in OLSR, it has a benefit of knowing the routes immediately when needed. A pure link state routing protocol has the characteristic that all the links with neighbor nodes are declared and are broadcast to the whole network. However, since OLSR is the optimization of the link state routing protocol for an ad hoc network, it uses the reduced size of control packets, declaring only a subset of links with its neighbors who are its multipoint relay selectors, instead of all links. Besides, OLSR minimizes flooding of this control packet by using only the selected nodes, called multipoint relay, to disperse its messages in the network. The multipoint relay is the idea to diminish the flooding of broadcast packets in the network by lessening duplicate retransmission in the same region.

TBRPF [68] is a proactive, link-state routing protocol designed for mobile ad-hoc networks, which provides hop-by-hop routing along shortest paths to each destination. Each node running TBRPF computes a source tree (providing paths to all reachable nodes) based on partial topology information stored in its topology table, using a modification of Dijkstra's algorithm. To minimize overhead, each node reports only *part* of its source tree to neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reported part of its source tree. Each node also has the option to report additional topology information (up to the full topology), to provide improved robustness in highly mobile networks. TBRPF performs neighbor discovery using "differential" HELLO messages which report only *changes* in the status of neighbors. This results in

HELLO messages that are much smaller than those of other link-state routing protocols such as OSPF.

III. AD HOC ROUTING PROTOCOLS

3.1 Desirable Properties

If the conventional routing protocols do not meet our demands, we need a new routing protocol.

The question is what properties such protocols should have? These are some properties [5] that are desirable:

Distributed operation:

The protocol should be course be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The difference is that node in an ad hoc network can enter/leave the network very easily and because of mobility the network can be partitioned.

Loop Free:

To improve the overall performance, we want the routing protocol to guarantee that the routes supplied are loop free. This avoids any waste of bandwidth or CPU consumption.

Demand based operation:

To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. This means that the protocol should only react when needed and that the protocol should not periodically broadcast control information.

Unidirectional link support:

Bidirectional links are typically assumed in the design of routing algorithms. However, there are a number of factors that will cause wireless links to be unidirectional, including the presence of different radio capabilities and signal interference. Therefore, in situations where a pair of unidirectional links (in the opposite direction) forms the only bidirectional connection, the ability to make use of unidirectional links is considered valuable.

Security:

The radio environment is especially vulnerable to impersonation attacks, so to assure the wanted behavior from the routing protocol, we need some sort of preventive security measures. Authentication and encryption is probably the way to go and the problem here lies within distributing keys among the nodes in the ad hoc networks. There are also discussions about using IP-sec [A 14] that uses tunneling to transport all packets.

Power conservation:

The nodes in the ad hoc network can be laptops and thin clients, such as PDAs that are very limited in battery power and therefore uses some sort of stand-by mode to save power. It is therefore important that the routing protocol has support for these sleep-modes.

Multiple routes:

To reduce the number of reactions to topological changes and congestion multiple routes could be used. if one route has become invalid, it is possible that another stored route could still be valid and thus savings the routing protocol from initiating another route discovery procedure.

Quality of service support:

Some sort of Quality of Service support is probably necessary to incorporate into the routing protocol. This has a lot to do with what these networks will be used for. It could for instance be real-time traffic support.

Efficient utilization of bandwidth:

If as routing protocol incurs excessive control traffic, the available network bandwidth will be consumed by control traffic. This can impact communication performance. Since the bandwidth of a wireless network is limited, reduction of control overhead is an important design factor.

3.2 Categorization of Ad hoc Routing Protocols

Numerous protocols have been developed for ad hoc mobile networks to deal with the typical limitations of these networks, which include high power consumption, low bandwidth, and high error rates. As shown in Figure below, these routing protocols [5, 63] may generally be categorized as:

- ✓ **Proactive or Table-driven Routing Algorithms**
- ✓ **Reactive or On-demand Routing Algorithms**

Solid lines in this figure represent direct descendants, while dotted lines depict logical descendants. Despite being designed for the same type of underlying network, the characteristics of each of these protocols are quite distinct.

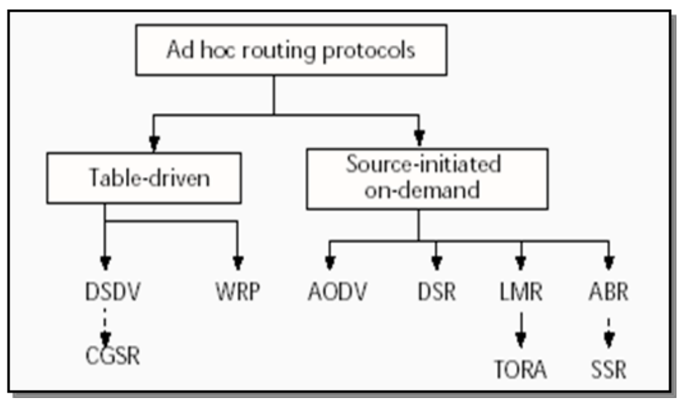


Figure 2.2 Categorization of Mobile Ad Hoc Routing Protocol

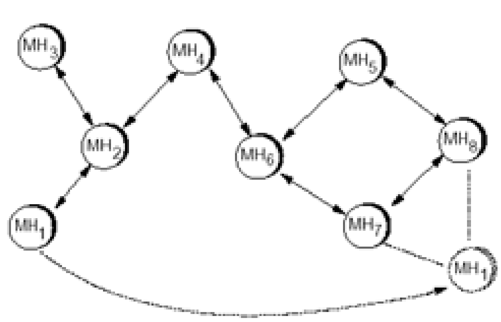
3.3 Proactive or Table-driven Routing Algorithms

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view or we can say that Proactive routing algorithms are those in which each node knows the full topology network view at every time . In this type of algorithms, routing is continuously updated regardless of the traffic activity in the network. These algorithms have the important feature of low latency in routing a packet, because routing algorithm is always ready. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast.

3.3.1 Destination-Sequenced Distance Vector Routing (DSDV):

DSDV [17] is a table driven algorithm based on modification made to the Bellman-Ford routing mechanism. Each node in the network maintains a routing table that has entries for each of the destination in the network and the number of hops required to reach each of them. Each of the entry has a sequence number associated with it that helps in identifying stale entries. Thus avoiding formation of routing loops. Each node periodically sends updates tagged through out the network with a monotonically increasing even sequence number to advertise its location. New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. The route labeled with the most recent sequence number is always used. Once its neighbors receive this update they recognize that they are one hop away from the transmitting node and include this information in their distance vectors. Every node stores the “next routing hop” for every reachable destination in their routing table. The route used is the one with the highest sequence number i.e. the most recent one. When a neighbor **B** of **A** finds out that **A** is no longer reachable, it advertises the route to **A** with an infinite metric and a sequence number one greater than the latest sequence number for the route, forcing any nodes, with **B** on the path to **A**, to reset their routing tables.

Since each update is broadcasted to the entire network, there is a potential of causing large network traffic. To alleviate this problem, updates employ two possible types of packets: “full dump” and “incremental”. In case of *full dump*, packet carries all available routing information and can require multiple network protocol data units (NPDU). During periods of occasional movement, these packets are transmitted infrequently. The smaller *incremental* packets are used to relay only that information which has changed since the last full dump. Each of these broadcasts requires that the packets fit into a standard-size NPDU, thereby decreasing the amount of traffic generated.



Destination	Metric	Sequence number
MH_1	2	S406_MH_1
MH_2	1	S128_MH_2
MH_3	2	S564_MH_3
MH_4	0	S710_MH_4
MH_5	2	S392_MH_5
MH_6	1	S076_MH_6
MH_7	2	S128_MH_7
MH_8	3	S050_MH_8

Advertised route table by MH_4

Destination	Metric	Sequence number
MH_4	0	S820_MH_4
MH_1	3	S516_MH_1
MH_2	1	S238_MH_2
MH_3	2	S674_MH_3
MH_5	2	S502_MH_5
MH_6	1	S186_MH_6
MH_7	2	S238_MH_7
MH_8	3	S160_MH_8

MH_4 advertised table (updated)

Figure 2.3 Movement in Ad Hoc Network and the table updates.

3.3.2 The Wireless Routing Protocol:

The Wireless Routing Protocol (WRP) described in [18] is a table-based protocol with the goal of maintaining routing information among all nodes in the network

WRP belongs to the class of path finding algorithms with an important exception. It avoids the “count to infinity” problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This is a table driven routing protocol which maintains the routing information among all nodes in the network, each nodes in the network contains the four tables:

1. Distance table
2. Routing table
3. Link cost table
4. Message Re-transmission List (MRL)

Each entry of the MRL contains the sequence number of the update message, a retransmission counter, an acknowledgement requested flag vector with one entry per neighbor and a list of updates message mobiles inform to each of link changes through the use of update message. An update message contains a list of updates. Mobiles send the update messages after processing updates from neighbors or detecting a change in a link to a neighbor. In the event of the loss of a link between two nodes, the nodes send update messages to their neighbors. The neighbors then modify their distance table entries and check for new possible paths through other nodes. After getting the acknowledgements and other messages the nodes know the existence of their neighbors. If a node is not sending any message then that node will send a hello message to ensure the connectivity with other nodes otherwise, No message from the node will indicate the failure of the link. On the other hand if a node receives a hello message from any other node then this new node is added to the routing table of table of that mobile node and this mobile node sends a copy of its routing table information to the new node. WRP is a loop free algorithm. In WRP routing nodes communicates the distance and second to last hop information for each destination in the wireless network. This is the reason that WRP is known as the path finding algorithm.

3.3.3 Cluster head Gateway Switch Routing:

This CGSR [53] protocol is different from the DSDV according to the addressing and the network organization scheme. CGSR is a clustered multi hop mobile wireless network with several heuristic routing schemes[15] instead of flat network. A CGSR algorithm is utilized to elect a node as the cluster head using a distributed algorithm within the cluster. But the main disadvantage of this CGSR algorithm is that its cluster head selection rather than packet relaying. To remove this problem a least cluster change algorithm (LCC) is introduced. Using LCC, cluster heads come into contact of all other cluster heads. CGSR uses the DSDV as the underlying routing scheme, and hence has much of the same overhead as DSDV, however it modifies DSDV by using a hierarchical cluster head to gate way routing approach to route traffic from Source to destination. Gateways nodes are called these type of nodes that are within communication range of two or more cluster head and then the packet is routed from the cluster head to the gateway node to another cluster head and so on until the cluster head of the destination gateway (node) is reached. Using this algorithm each node must keep a “cluster member table “where it stores the destination cluster head for each mobile node in the network. These cluster member tables are broadcast by each node periodically using the DSDV algorithm. Nodes update their cluster member tables on reception of such a table from a neighbor.

In CGSR each node must also maintain a routing table which is used to determine the next hop in order to reach the destination. On receiving a packet a node will consult its cluster member table and routing table to determine the nearest cluster head along the route to the destination next, the node will check routing table to determine the next hop used to reach the selected cluster head, It then transmits the packet to this node.

3.4 Reactive or On-Demand Routing Algorithms

A different approach from table-driven routing is reactive routing algorithms or source-initiated on-demand routing [62]. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. This type of algorithms tries to minimize routing traffic but latency may be performed before sending a packet. The Reactive routing algorithms are following:

3.4.1 AODV (Adhoc on Demand Vector Routing Protocol):

AODV algorithm described in [55] is based upon the DSDV or we can say that AODV is an improvement on DSDV because in DSDV algorithm a complete list of the routes from the source to the destination is maintained by a source node on the other node it minimizes the number required broadcasts by creating routes on the demand basis. So AODV is known as the pure On Demand routing algorithm.

In AODV, when a node wants to send a message to some destination node and this source node does have not any route to that destination node then it uses a path discovery process. It broadcasts a route request message (RREQ) to its neighbors, which then forward the request to their neighbors and this process is continues until the destination node is reached. To remove the problem of the looping AODV utilizes the destination sequence numbers and contain the most recent route information. Each node contains its own sequence number, as well as each node contains a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates and together with the node’s IP address. 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. Once the RREQ reaches at the destination then the intermediate nodes responds by sending a route reply RREP packet back to the neighbor from which it first received the RREP. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their tables which point to the node from which the RREP came. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links.

AODV is also known as for the route maintenance. The route maintenance by AODV is done in the following way. 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 neighbor notices the movement and broadcasts a link failure notification message to neighbor node to inform them of the erasure of that part of the route and this node prorogates this link failure notification to their neighbors and this process is continued until the source node is reached. Now this source node may choose the route discovery process for the destination if a route is still needed by the source node.

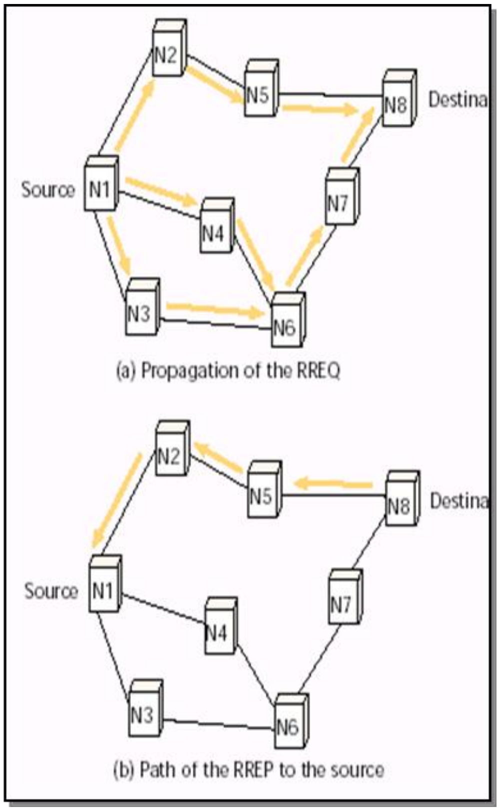


Figure 2.4 AODV Route Discovery

3.4.2 Dynamic Source Routing (DSR)

DSR [20, 54] uses source routing i.e. the packet contains the full route to destination and the intermediate nodes do not have to make any routing decisions. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which to forward the packet; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. DSR has two principal components: Route Discovery and Route Maintenance. A ROUTE REQUEST packet is used for Route Discovery. A ROUTE REPLY packet answers this from the destination or a connected node. To reduce the overhead for Route Discovery, nodes maintain a cache of learnt or overheard routes. Route Maintenance is the mechanism used to detect link failures and a ROUTE ERROR packet is used to notify the sender. The sender can then use another route stored in its cache or initiate Route Discovery.

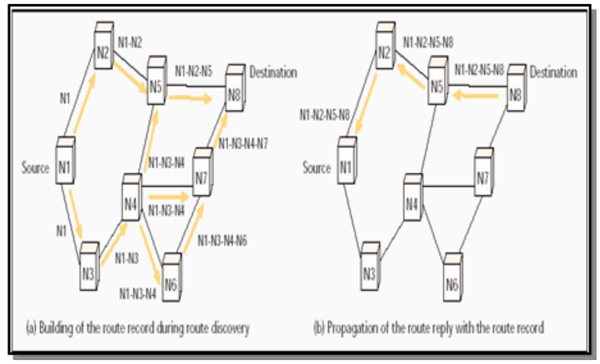


Figure 2.5 Creation of a route record in DSR

In Distance vector and link state routing, a host must continue to send advertisements even when nothing changes, so that other mobile hosts will continue to consider those routes or network links as valid. Unlike the case in conventional routing protocols, in DSR, there are no periodic router advertisements involved. Instead, the routing information is cached in the routing tables at the host and when a host needs to route a packet to another host, it dynamically determines the route based on the cached information. Since there are no periodic advertisements involved, it results in reducing network bandwidth overhead; in particularly during periods when little or no significant host movement involved i.e. no change in the routing information. Battery power is also conserved on the mobile hosts, both by not sending the advertisements and by not needing to receive them. Thus a host could reduce its power usage by putting itself into "sleep" or "standby" mode when not busy with other tasks.

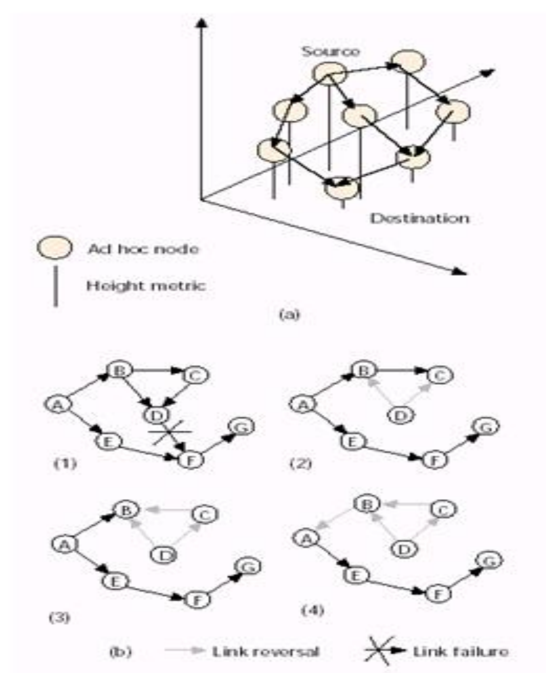


Figure 2.6 (a) Route Creation & (b) Route maintenance in TORA

3.4.3 Temporally Ordered Routing Algorithm (TORA)

It is a distributed routing protocol [57]. The basic underlying algorithm is in a family referred to as to as link reversal algorithm. TORA [61] is designed to minimize reaction to topological changes. A key concept in its design is that control messages are typically localized to a very small set of nodes. It guarantees that all routes are loop free and typically provides multiple routes for any source/destination pair. It provides only the routing mechanism and depends on Internet MANET Encapsulation Protocol for other underlying functions.

TORA [56] can be separated into three basic functions which are creating routes, maintaining routes, and erasing routes. The creation of routes basically assigns directions to links in an undirected network or portion of the network, building a directed acyclic graph (DAG) rooted at the destination

TORA associates a height with each node in the network. All messages in the network flow downstream from a node with higher to a node with lower height. Routes are discovered using Query (QRY) and Update (UPD). When a node with no downstream links needs a route to a destination, it will broadcast a QRY packet. This QRY packet will propagate through the network until it reaches a node that has a route or the destination itself. Such a node will then broadcast a UPD packet that contains the node height. Every node receiving this UPD packet will set its own height to a larger height than specified in the UPD message. The node will than broadcast its own UPD packet. This will result in a number of directed links from the originator of the QRY packet to the destination. This process can result in multiple routes.

Maintaining routes refers to reacting to topological changes in the network through in the network in a manner such that routes to the destination are re-established within a finite time, meaning that its directed portions return to a destination –oriented graph within finite time. Upon detection of a network partition, all links in the portion of the network that has become partitioned from the destination are marked as unidirectional ton erase invalid routes. The erasing of routes is done using clear (CLR) messages.

3.4.4 Associativity Based Routing Protocols:

This is totally different routing protocol for adhoc wireless network. ABR protocol is totally free from loops, deadlocks and packet duplication and it defines a new routing metric for ad hoc mobile ad hoc network and this type of network is known as the degree of the association stability. In this protocol each node has its degree of association stability and each node in the network is selected based on its degree of association stability. In this protocol each node generates a beacon to signify its existence and when this is received by neighboring nodes then due to this beacon the associativity table id updated. So we can say that for each beacon received the associativity tick of the current node with respect to the beaconing node is incremented. Association stability is defined by connection stability of one node with respect to another node over time and space. If any node contain a high degree association stability then it indicates the node contain a low mobility on the other hand a low degree indicates a high state of node mobility. There are three phases of ABR which are following:

1. Route Discovery
2. Route Reconstruction
3. Route Erasure

First phase is done by broadcast query and wait reply cycle. A node which wants to create a route, broadcasts a BQ messages to the nodes that have a node to the destination. All nodes which receive this message append their address and their associativity ticks with their neighbors along with QoS information to the query packet. In this way each resultant packet arrives at the destination. The destination is then able to select the best route by examining the associativity ticks along each of the paths. But when multiple paths have the same degree of association stability then in this condition the route with the minimum number of hops is selected. After the entire destinations send a REPLY packet back to the source along this path. Nodes which contain the REPLY packet are considered as the valid nodes for the route from source to the destination. RRC may consist of partial route discovery, invalid route erasure, valid route updates and new route discovery depending on which node along the route move. In ABR protocol when a discovered route is no longer desired the source node initiates a route delete (RD) broadcast so that all nodes 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 RRL.

3.4.5 Signal Stability Routing Protocol:

The best On-demand routing protocol is the signal stability based routing protocol [59] (SSR) .Unlike the algorithm which we have studied, SSR selects the routes based on the signal strength between any node and its neighbor. We can say that the nodes which have the strongest connectivity are choused for the route. The SSR can be divided into two corporate protocols

1. **Dynamic Routing Protocol(DRP)**
2. **Static Routing Protocol(SRP)**

DRP is responsible for the maintenance of signal stability & routing table (RT). The SST contains the signal strength of neighboring nodes and these signal strength are recorded as either a strong channel or week channel. So all transmissions are received & processed in the DRP. After updating all appropriate table entries, the DRP passes a received packet to SRP.

IV. REACTIVE VS. PROACTIVE AD HOC ROUTING PROTOCOLS

Most routing protocols in mobile ad hoc networks derive from distance vector or link state algorithms [60, 69].

In distance vector routing [18], each router maintains a table containing the distance from itself to all possible destinations. Each router periodically transmits this table information to all its neighbor routers, and updates its own table by using the values received from its neighbors. Based on the comparison of the distances obtained from its neighbors for each destination, a router can decide the next hop as the shortest path from itself to the specified destination. When each router has a packet to send to some destination, it simply forwards the packet to the decided next hop router. When the routing table is frequently updated, the algorithm speeds up the convergence to the correct path. However, the overhead in CPU time and network bandwidth for flooding routing updates also increases. Perkins and Bhagwat [Perkins1994] devised a Destination-Sequenced Distance Vector (DSDV) protocol based on the classical Bellman-Ford routing algorithm to apply to mobile ad hoc networks. DSDV also has the feature of the distance-vector protocol in that each node holds a routing table including the next-hop information for each possible destination. Each entry has a sequence number. If a new entry is obtained, the protocol prefers to select the entry having the largest sequence number. If their sequence number is the same, the protocol selects the metric with the lowest value. Each node transmits advertisement packets using increasing sequence numbers [Perkins1994]. A study of performance evaluation on DSDV [Broch1998] shows that DSDV is able to deliver virtually all data packets when each node moves with relatively low speed. However, when the mobility of each node increases, the speed at which the system converges to the correct path decreases [Broch1998].

While DSDV is a proactive protocol that always tries to maintain the correct information regarding network topology, Ad hoc On-demand Distance Vector (AODV) [Perkins1999] is a reactive protocol to perform Route Discovery only when a new route needs to be found. Thus, AODV does not maintain any routing information nor transmit any periodic advertisement packets for exchanging routing tables. That is, only when two nodes need to communicate with each other, will they forward routing packets to maintain connectivity between the two nodes. Usually, when there is a need for communication between two nodes, each mobile node transmits a local broadcast packet known as a hello message. Routing tables of the nodes within the neighborhood are organized for the optimization of response time to local movements and the support of rapid response time for requests to establish a new route. AODV is similar with the Dynamic Source Routing (DSR) protocol; however, while DSR is based on source routing, AODV is dependent upon dynamically establishing route table entries at intermediate nodes.

In addition to the viewpoint categorizing routing protocols in terms of either distance vector or link state routing, routing protocols for ad hoc networks also can be classified as reactive routing protocols versus proactive routing protocols, as mentioned previously. In the reactive routing approach, a routing protocol does not initiate Route Discovery until it is needed. The protocols only attempt to find a route to a destination totally based on demand. Examples of reactive routing protocols for ad hoc networks include AODV [5], DSR [20], and TORA [18]. On the contrary, the proactive routing approach is based on the exchange of knowledge of network topology periodically. The proactive protocols provide a needed route instantly at the expense of bandwidth because of transmitting periodic updates of topology frequently. Examples of proactive routing protocols include DSDV, STAR, and TBRPF etc.

CONCLUSIONS

We have studied several existing routing protocols and adhoc wireless networks and found that no single routing algorithm is the solution for the same. The fuzzy metric approach improves the performance compared with the other approach used traditionally in the routing technique. The proposed approach offers the improvement schemes with its features such as it yields loop free routes, helps in multi path routing, gives the faster response at low overheads and the overall evaluation is positive in the sense that we applied an intelligent algorithm for inferring statistically the internal state of the network, and the outcome was surprisingly accurate. The results of the proposed routing algorithm confirm that the protocol presents a considerable reduction of routing overhead, whereas the overall performance is competitive with other protocols.

REFERENCES

[1] Ashwani Kush, Phalguni Gupta, Ram Kumar, "Performance Comparison of Wireless Routing Protocols", Journal of the CSI, Vol.35 No.2, April-June 2005

[2] Anne Aaron, Jie Weng, "Performance Comparison of Ad-hoc Routing Protocols for Networks with Node Energy Constraints", available at http://ivms.stanford.edu

[3] Charles Perkins, Elizabeth Royer, Samir Das, Mahesh Marina,"Performance of two on-demand Routing Protocols for Ad-hoc Networks", IEEE Personal Communications, February 2001, pp.16-28.

[4] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[5] C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA,1999, pp. 90-100.

[6] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers", Proceedings of ACM SIGCOMM 94, 1994, pp. 34–244.

[7] D. Bertsekas and R. Gallager, "Data Networks" Prentice Hall Publ., New Jersey, 2002.

[8] D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003, work in progress. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[9] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer Publ., 1996, pp. 152-81.
[10] David A. Maltz, “On-Demand Routing in Multi-hop Wireless Mobile Ad Hoc Networks’, May 2010, available at www.monarch.cs.rice.edu
[11] E.M.Rover, C.K.Toh, “A review of current routing protocols for ad hoc networks”, IEEE Communications, vol 6, 1999, pp 46-55.
[12] F. Bertocchi, P. Bergamo, G. Mazzin, “Performance Comparison of Routing Protocols for Ad hoc Networks”, IEEE GLOBECOM 2011.
[13] Farhat Anwar, Md. Saiful Azad, Md. Arafatur Rahman, Mohammad Moshee Uddin, “Performance Analysis of Ad hoc Routing Protocols in Mobile WiMAX Environment”, IAENG International Journal of Computer Science, 35:3, IJCS_35_3_13
[14] H. Ehsan and Z. A. Uzmi (2004), “Performance Comparison of Ad HocWireless Network Routing Protocols”, IEE,E 8th International Multitopic Conference, Proceedingsof INMIC, December 2004, pp.457 – 465.
[15] Iskra Djonova Popova, “A PowerPoint presentation on Routing in Ad-hoc Networks”, 9th CEENet Workshop on Network Technology, Budapest 2010.
[16] J. Broch, D.A. Maltz, D. B. Johnson, Y-C. Hu, J. Jetcheva, “A performance comparison of Multi-hop wireless ad-hoc networking routing protocols”, in the proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM ’98), October 1998, pages 85-97.
[17] Wang, K. Ren, W. Lou, and J. Li, “Towards publicly auditable secure cloud data storage services,” IEEE Network Magazine, vol. 24, no. 4, pp. 19–24, 2010.
[18] M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.
[19] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.
[20] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS ’09), pp. 1 -9, July 2009.
[21] Arjun Kumar, Byung Gook Lee, HoonJaeLee “Secure Storage and Access of Data in Cloud Computing” 2Department of Computer and Information Engineering Dongseo University, Busan, 617-716, Korea.
[22] C. Wang, K. Ren, W. Lou, and J. Li, “Toward publicly auditable secure cloud data storage services,” IEEE Vol 24, no. 4, pp. 19–24, 2010