A Simulation Study of Routing Algorithm of Mobile Ad hoc Networks

Akshai Aggarwal, *Senior Member, IEEE,* Savita Gandhi, *Senior Member, IEEE and* Nirbhay Chaubey, *Member, IEEE*

***Abstract*--Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). A mobile ad hoc network (MANETs) is a collection of mobile nodes which establishes the Network spontaneously and communicate over a shared wireless channel without any pre-existing infrastructure and central administration. The absence of central authorization facility in a dynamic and distributed environment requires collaboration among nodes. Mobile nodes, which want to communicate with each other over a wireless communication medium, act as both host and routers to forward packets to everyone. Secure routing in MANETs is an area of active research. This paper describes existing MANETs routing algorithm and compares these protocols. It provides a detailed study of two routing protocols Zone Routing Protocol (ZRP) and Optimum Link State Routing Protocol (OLSR). The paper then proposes a new routing algorithm, which provides all the features available in ZRP and OLSR and which may work more efficiently than the existing protocols.**

***Index Terms*-- Ad hoc networks, MANET, routing protocols, proactive routing protocols, reactive routing protocols**

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are a heterogeneous mix of different wireless and mobile devices, ranging from little hand-held devices to laptops that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis [1]. There are some unique characteristics of mobile ad hoc networks [2], [8]-[10].

First, the connections between network nodes are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and form a network, not necessarily with any assistance from the cable connections.

Second, unlike traditional wireless networks, mobile ad hoc networks do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing; the execution context is extremely dynamic.

Third, the membership is always changing. The mobile nodes are free to move anywhere, leave at any time and new nodes can enter unexpected.

Fourth, the execution environment is insecure and unfriendly. Due to the lack of fixed infrastructure and administration, there are increased chances that malicious nodes can mount attacks.

Finally, the nodes in a mobile ad hoc network are usually portable mobile devices with constrained resources, such as power, computation ability and storage capacity.

Given the limited range of wireless communication, the network is generally multihop, since direct communication between mobiles is generally not available. For this reason, a distributed routing protocol is required in order to provide communication between arbitrary pairs of nodes. A major problem arises from the mobility of nodes causing the network topology to be variable and to some extent unpredictable. In fact, communication links between nodes may be broken, nodes may fail and possibly recover from failures and new links may appear. The routing protocol must react promptly to recover from link and node failures and to take advantage of new links. For these reasons, existing routing protocols designed for fixed networks are unsuitable, and routing in ad hoc networks is a major issue.

Mobile ad hoc networks are highly applicable to environment in which no fixed infrastructure is available, either because it may not be economically practically possible to provide the necessary infrastructure or because the expediency of the situation does not permit its installation, such as emergency deployments, disasters, search and rescue missions and military operations [5]. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as virtual classrooms etc.

Akshai Aggarwal is a Director, School of Computer Science, University of Windsor.

Savita Gandhi is a Professor & Head at the Department of Computer Science, Gujarat University.

Nirbhay Chaubey is Lecturer of Computer Science at Institute of Science and Technology for Advanced Studies and Research, Gujarat, India

II. ROUTING PROTOCOLS

Routing protocols for wireless ad hoc networks can be mainly classified into the three categories of Table-driven (or Proactive) [2], [4] [8], [9], [17], [18] On-demand (or Reactive) [3], [6], [10]-[14], [19],[21] and Hybrid Routing Protocol [20].

A. Pro-active Routing (Table-driven)

Table driven ad hoc routing protocols maintain at all times routing information regarding the connectivity of every node to all other nodes that participate in the network. Also known as proactive, these protocols allow every node to have clear and consistent view of the network topology by propagating periodic updates. Therefore, all nodes are able to make immediate decisions regarding the forwarding of a specific packet. The main disadvantages of such algorithms are –

i. Respective amount of data for maintenance.
ii. Slow reaction on restructuring and failures.

1. *Destination Sequenced Distance Vector (DSDV):*

This algorithm uses routing table like Distance vector but each routing table entry is tagged with sequence number, generated by destination. To maintain consistency among routing tables in a dynamically varying topology updates are transmitted periodically. Each mobile station advertises its own routing table to its current neighbors [4].

Routing information is advertised by broadcasting or multi casting. Packets are transmitted periodically and incrementally as changes are detected. In a wireless medium broadcasts are limited by the physical characteristic of medium. If a node invalidates its entry to a destination due to loss of next hop node, increments its sequence number and uses new sequence no in its next advertisement of the route. Data broadcast by each mobile computer will contain new sequence number and.

i. Destination IP address
ii. Number of hops required reaching the destination
iii. Sequence number of the information received regarding that destination

Routes with more recent sequence number are preferred but if routes have same sequence number route with lower metric is preferred.

To reduce the information carried in broadcast two types exist

i. Full dump carry all the available routing information
ii. Incremental carry only changed information since the last full dump.

Broadcast is an asynchronous event. It may happen that every time a mobile host receives a worse metric than the upcoming sequence number update. In that case, route to destination change at every new sequence number. Solution to this is to delay the advertisement. If mobile host can determine that route with better metric is likely to show up soon. For this two routing tables are maintained, one for forwarding packets and other for incremental routing information packets. DSDV guarantees a loop free path to each destination without requiring nodes to participate in any complex update coordination protocol. In this routing tables of each node can be visualized as forming N trees, one rooted at each destination. Its space complexity is O (n).

2. *Distance Vector Routing Algorithm:*

In this each router maintains the information about all other routers through a routing table.

Routing table has following entries

i. Destination IP address
ii. Distance
iii. Next hop in path

Each router periodically broadcasts this table to its neighbors. This routing algorithm is computationally more efficient, easier to implement and require much less storage space but it can cause formation of short as well as long lived loops. Loops are formed because nodes choose their next hop in a completely distributed fashion based on the information which can possible be stale. Looping problem can be solved using poisoned reverse technique. This can solve the problem only if loop has three nodes, if a loop has more than three nodes (count to infinity problem), poisoned reverse won't work.

In poisoned reverse, in a loop of three nodes, source node will advertise its direct distance to destination node as infinity till it uses via path. Inter nodal coordination protocol can also be used to remove looping problem but due to more topological changes in wireless network, it does not work. Poisoned reverse does not work because of broadcast nature of transmission medium. We need to have the routing algorithm, which preserves the simplicity of Distance Vector algorithm as well as avoids looping problem [12].

3. *Efficient Ad hoc Distance vector routing (SEAD):*

Hu, Perrig and Johnson presented a table driven routing protocol, Secure Efficient Ad hoc Distance vector routing (SEAD) [17], [18] which is based on Destination-Sequence Distance Vector Protocol (DSDV) [4].

In distance vector routing, each route maintains a routing table listing all possible destinations within the network. Each entry in a node's routing table contains the address of some destination, this node's shortest known distance to that destination, and the address of the node's neighbour that is the first hop on this shortest route to that destination. To maintain the routing table, each node periodically transmits a routing update to each of its neighbour routes, containing the information from its own routing table. A node also uses triggered updates, in which a node transmits a new update about some destination as soon as the metric in its table entry for that destination changes, rather than waiting for its next scheduled periodic update to be sent. The updates may be either a “full dump”, listing all destinations, or an “incremental” update, listing only destinations for which the route has changed since the last full dump sent by that node.

SEAD uses efficient one-way hash chain rather than relying on expensive asymmetric cryptography operations. Especially on CPU-limited devices, symmetric cryptography operations are three to four orders of magnitude faster than asymmetric operations. SEAD assumes some mechanism for a node to distribute an authentic element of the hash chain that can be used to authenticate all the other elements of the chain. SEAD does not cope with colluding attacks, such as wormhole attack.

4. *Optimal Link state Routing Protocol (OLSR):*

OLSR is a routing protocol designed for wireless mobile ad-hoc networks. OLSR was proposed with inria that was National Research Institute in France. It operates as a table driven, proactive protocol and utilizes a technique called multipoint relaying for message flooding, thus exchanges topology information with other nodes of the network regularly. The nodes which are selected as a multipoint relay (MPR) by some neighbor nodes announce this information periodically in their control messages. Thereby, a node announces to the network, that it has reachability to the nodes which have selected it as MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. OLSR which uses the stability of link state protocol but reduces the size of packet as well as flooding using multi point relays. This works in distributed manner and maintains path to every destination. It performs hop-by-hop routing i.e. each node uses most recent information to route the packet. It uses control messages in order to trace nodal mobility. OLSR performs following actions in order to reduce the control traffic and flooding

i. Efficient Neighbor Sensing
ii. Efficient Flooding of Control Traffic
iii. Efficient Sensing of Topological Changes

To sense its neighbors each node emits a HELLO packet periodically which consists of it’s own address and link status of all its neighbors. Link status depicts the type of link between two nodes, which can be unidirectional, bi-directional or Multi Point Relay. With the help of these HELLO packets each neighbor maintains information about its immediate and two hop neighbors in the neighbor table. On the basis of neighbor table MPR selection is performed. A link is bi-directional if a node finds its own address in a received HELLO packet. To get the information about all the nodes in the network a node emits control messages, which will be flooded in the entire network in such a way that a node receives a particular packet only once. This is done using MPR. Multi point relay is a technique to reduce the number of duplicate transmissions while forwarding a broadcast packet. This technique limits the retransmission to the limited set of neighbors called multi point relay. In this each node independently calculates its own set of multi point relays in a distributed fashion. With the change of neighbor MPR set changes [13]-[15]. MPR set selection is based on neighbor sensing technique through which a node has the information about its one hop and two hop neighbors. For a node x, say, set of one hop neighbors N (x), set of two hop neighbors N’ (x), selected multi point relay set MPR (x).

i. Select all the nodes which are the neighbor of some node in N’ (x) from N (x) and add them to MPR (x) set.
ii. Now, for each node in N (x) which is not the part of MPR (x) find out number of nodes in N’ (x) which it covers among the uncovered nodes. Add the node to MPR (x) for which this number is largest.

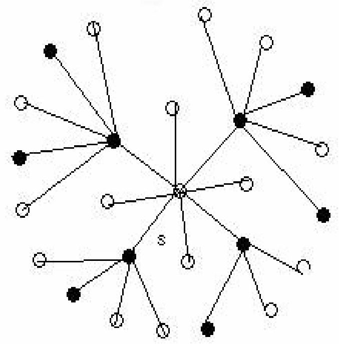

Fig. 1. Shows Diffusion of Broadcast Message using Multi Point Relays.

Nodes, which consist of MPR selector set, generate TC (Topology Control) message, which consists of its own address and address of all MPR selectors of that node and sequence number of MPR selector set. Thus it defines the reach ability of a node to all its MPR selectors. This mechanism helps each node to generate its topology table. Node with empty MPR selector may not emit TC messages. Topology table of each node consists of information about multi point relays of other nodes based on which routing table is formed. Topology Table has following fields

i. Destination address (MPR selector in received TC message)
ii. Address of last hop node to destination (originator of TC message)
iii. MPR selector set sequence number (of the sender node)

Parsing and storing TC messages in form of last hop, node in the descending order build routing table. Routing Table depends on both topology table and neighbor table. If any one of these changes routing table need to change. It consists of

i. Destination Address
ii. Next Hop Address
iii. Estimated Distance to Destination

To recalculate routing table

i. Remove all the entries of routing table
ii. Record all bi-directional entries starting from one hop neighbor
iii. If destination address in topology table does not correspond to destination address of any route entry routing table and its last hop address corresponds to destination address of a route entry with distance equal to h then a new route entry is done which has destination as destination in topology table, next hop as last hop (described above), distance as h+1.
iv. Remove unnecessary entries from topology table.

B. Reactive Routing (On-demand)

Reactive routing protocols, which appear to be more suitable for ad hoc networks, do not maintain up-to-date information about the network topology as it is done by the proactive ones, but they create routes on demand. Among reactive routing protocols, the Dynamic Source Routing (DSR) [6] and the Ad hoc On Demand Distance Vector Routing (AODV) [19] are the most established developments. This type of protocols finds a route on demand by flooding the network with Route Request packets.

1. *Ad hoc On Demand Distance Vector (AODV):*

In AODV, routes are set up by flooding the network with RREQ packets which, however, do not collect the list of the traversed hops. Rather, as a RREQ traverses the network, the traversed mobiles store information about the source, the destination, and the mobile from which they received the RREQ. The latter information is used to set up the reverse path back to the source. When the RREQ reaches a mobile that knows a route to the destination or the destination itself, the mobile responds to the source with a route reply packet which is routed through the reverse path set up by the RREQ, also setting the forward route from the source to the destination. To avoid overburdening the mobiles with information about routes which are no longer (if ever) used, nodes discard this information after a timeout [19].

2. *Dynamic Source Routing (DSR):*

In DSR, when a mobile (source) needs a route to another mobile (destination), it initiates a route discovery process which is based on flooding. The source originates a route request (RREQ) packet that is flooded over the network. The RREQ packet contains a list of hops which is collected by the route request packet as it is propagated through the network. Once the RREQ reaches either the destination or a node that knows a route to the destination, it responds with a route reply (RREP) along the reverse of the route collected by the RREQ [6]. This means that the source may receive several RREP messages corresponding, in general, to different routes to the destination. DSR selects one of these routes (for example the shortest), and it maintains the other routes in a cache. The routes in the cache can be used as substitutes to speed up the route discovery if the selected route gets disconnected. To avoid that RREQ packets travel forever in the network, nodes that have already processed a RREQ discard any further RREQ bearing the same identifier.

The main difference between DSR and AODV is in the way they keep the information about the routes: in DSR it is stored in the source while in AODV it is stored in the intermediate nodes. However, the route discovery phase of both is based on flooding. This means that all nodes in the network must participate in every discovery process, regardless of their potential in actually contributing to set up the route or not, thus increasing the network load.

III. Hybrid Routing Protocols

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases.

1) Zone Routing Protocol (ZRP):

ZRP is Hybrid routing protocol of MANET and more specifically ZRP limits the proactive phase of the protocol to the local neighborhood, while it uses the reactive phase to search units that are not in the local neighborhood. In ZRP, a unit proactively maintains routes to destinations within its local neighborhood [20].

Advantages of ZRP

i. Proactive technique is limited to node's local neighborhood.
ii. Search is performed by efficiently querying the selected nodes.
iii. Multiple free loop paths are identified from source to destination that increases the reliability

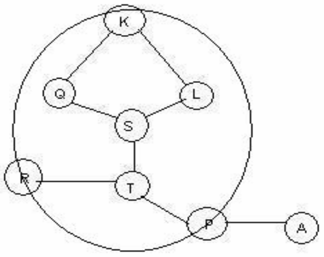

Fig. 2. Shows A routing zone of radius two hops:

In the figure above if destination is node P, sending packet is not a problem but if destination is node A inter zone routing mechanism is required and performance.

iv. Routing is flat, hence no network congestion.
v. It's behavior is adaptive.

Zone is a nodal connectivity not the physical distance between nodes. A zone of radius 'R' for a node contains all the nodes that are at max at the distance of 'R' hops from that node. A node is supposed to propagate updates only within its routing zone. A node learns the zone through some proactive scheme like Intra Zone Routing Protocol. Within the zone of a node sending a packet is not a problem.

What if destination is outside the zone of source node? We need Inter Zone Routing Protocol. In this source border cast a route request to all its peripheral nodes. They check whether destination is within their routing zone. If yes, fair enough and a route reply is sent back to the source. Else peripheral nodes forward the query further. This way it goes on. Every time a node appends its ID (may be IP address) to forwarded query. When destination is found accumulated sequence of these IDs specifies route between source and destination. IERP may generate more traffic than flooding because border casting limits the query propagation to zone radius. A node's query response maintains all the information about the entire zone of the particular node. To avoid this query detection and query termination are used. If query terminates only at peripheral nodes it may again cover the already covered area. To avoid this we allow terminating the query at intermediate nodes also called Early Termination. Intermediate nodes are not allowed to initiate the query. To implement Early Termination a node is supposed to know whether it belongs to previously detected zone or not.

Reconfigurable Wireless Network characteristics
Number of nodes: N
Node Density: d
Relative node velocity: v
Zone Radius: R

Control Overhead is independent from v and R. IARP route updates occur when there is change in network connectivity. Whenever a new neighbor is discovered or lost whole routing zone is updated by IARP.

Average node density = Average number of neighbors per node
Relative node velocity= Rate of new neighbor acquisition
These two parameters tell about the connectivity and changing topology of the network.

Control Traffic = IARP route update packets + IERP route/reply/failure packets
Control Overhead = Neighbor Discovery Beacons
IARP traffic / node / sec = v * IARP update traffic / neighbor (d, R)
IERP traffic = traffic generated per node * rate of query initiation = IERP traffic / query / node (d, R) * IERP query / sec = IERP traffic / query / node(d,R) * N * (Rinitialquery + Rsubsequentqueries)
Rsubsequentqueries = Route Discovering Rate = min(Rroutefailure(N,v,d,R), Rrouteusage)

If routes are used more often than they fail querying rate depends on network configuration, if route failures dominates querying rate dominates by behavior of user's application.

IERP traffic per query decreases with increase in zone radius. If R is constant amount of received traffic per query increases with zone density. Reception of query packets depends on the way of query propagation and this is independent from the size of network whereas amount of data carried by each packet depends on the size of network.

Rate at which queries are initiated depends on the route stability that in turn depends on node density, zone radius and node population. If node density is increased route stability increases and with the increase in zone radii route failure decreases because less connections need to be acquired. If node density and zone radii both are fixed and node population N is increased the length of path from source to destination increases in turn route reliability decreases. With the increase in node density both IARP route updates as well as IERP packets per query increases. If rate of queries are independent of route stability ZRP traffic increases with node density. Else if rate of query depends on route stability node density increases route reliability and decreases query rate.

Average node velocity is a measure of network reconfiguration. Higher node velocities result in linear increase in IARP routing zone updates and IERP route failures. Hence with v, ZRP traffic increases. For the efficient working of ZRP proper selection of zone radii is required. Optimal zone radius differs from network to network. Node density and relative node density can be measured by IARP but the parameters like route selection criteria, route caching policies and data traffic behavior are unpredictable.

Zone Sizing Schemes

i. Min Searching
ii. Traffic Adaptive

These are designed to minimize the control traffic using control traffic measurements only. In this zone radius is incremented/decremented by one hop until a radius is found for which ZRP traffic is minimum. Z(R (k)) denotes ZRP traffic when radius is k. If $Z(R(k)) <= Z(R(k-1))$, zone radius can be reduced further else reverse the direction. This process continues till $Z(R) <= Z(R-1)$ and Z(R)<=_ Z(R + 1).

What if ZRP traffic does not remain constant during the execution of min search? We need a mechanism that can adjust zone radius based on current ZRP traffic. If zone radius is less than optimal zone radius, ZRP traffic is dominated by IERP traffic and if zone radius is more than optimal zone radius ZRP traffic is dominated by IARP route updates.
T(R) = IERP traffic / IARP traffic
If T(R) < T threshold, increase R else decrease the R. This is traffic adaptive.

IV. Proposed Work

The proposal is to associate OLSR Multi Point Relays to the zone concept of ZRP. In OLSR we have multi point relays to forward updates i.e. only these Multi Point Relays have right to broadcast updates to the entire network. Multi Point relays can be at max two hops away. In ZRP a node routes the updates only within its zone. Zone Radius defines a zone. Zone Radius may be of any size. In case of inter zone routing mechanism only peripheral nodes can forward the packets within their zone. In this case there is no requirement of any zone sizing scheme because zone radius will be of maximum two hops only as Multi Point Relay are selected from two hops neighbors only. If we create a zone of multi point relays only having zone radius two because with the increase in zone radius IERP query traffic reduces and we can have at max two and route a packet according to intra and inter zone routing mechanisms, it may reduce the OLSR control traffic and require less bandwidth. With this zone radius become fixed and lesser number of Multi Point Relays may result in reduction of amount of traffic as fewer number of nodes will carry the traffic and it may become easier to control retransmission of packets. If zone radius is fixed received traffic depends only on node density and in our case it will depend only on the Multi Point Relays density.

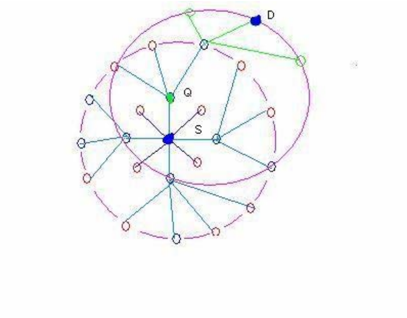

Fig. 3. Shows A routing zone of radius two hops of MPR:

In the figure above if source is s and destination is d, first s will find out it's MPR and then a zone of two hops including these MPR forms. Now, d does not lie within s zone so peripheral MPR will forward the query further and s lies in the zone of q.

V. Experimental Work and Results

We created a test-bed for performance analysis of various ad hoc routing protocols described in this paper. We formed a wireless ad hoc network using wireless adapters for emulate and ensured the connectivity among all the nodes. For the analysis of routing protocol we used a tool called "oolsr" provided by [22]. This is a complete implementation of OLSR in C++. We executed this code treating each node as a router. This is supposed to create "windows.obj" file but there is some linking problem.

By using the tool provided by [23] we generated results in the created testing environment. This is the OLSR implementation for MANET, which makes use of MPR, HELLO, messages, TC messages. Basically HELLO messages are used to learn about immediate neighbors of a particular node. But to learn about complete network we require TC messages. In this implementation HELLO and TC messages are forwarded with the additional feature of LQ(Link Quality) and NLQ(Neighbor Link Quality) which provides the information how good the links are. The messages are called LQ HELLO messages and LQ TC messages respectively. With the help of link quality measurement a packet is being forwarded through best path and we have been able to achieve better delivery rate of packets and higher efficiency. The sample results are as shown in tables. Our IP address is 192.168.0.102 and we have three other nodes in the wireless ad hoc network.

TABLE I: LINKS

IP address	LQ	lost	total	NLQ	ETX
192.168.0.100	1.000	0	10	0.898	1.11
192.168.0.101	0.700	3	10	0.596	2.40
192.168.0.103	1.000	0	10	0.898	1.11

Table.1. provides the information about links, the quality of link between us and neighbor, number of packet lost and ETX(Expected transmission Count) which is defined as 1/NLQ*LQ. With the help of ETX we are able to achieve high delivery rate of packets because a route having minimal expected transmission counts is selected.

Table 2: NEIGHBORS

IP address	LQ	NLQ	SYM	MPR	MPRS
192.168.0.100	1.000	0.898	YES	YES	YES
192.168.0.101	0.700	0.596	YES	NO	YES
192.168.0.103	1.000	0.898	YES	YES	YES

Table.2. provides the information about neighbors whether the link is symmetric or not. If the link is not symmetric, packets can't be transferred. MPR denotes whether we selected the neighbor as MPR(Multi Point Relay) or not and MPRS(Multi Point Relay Selectors) denotes whether neighbor has selected us as MPR or not. A node will be able to forward the update in the network only if it is selected as MPR. Since node 192.198.0.101 has not selected us (192.168.0.102) as MPR, we are not allowed to forward packet sent by it whereas other nodes in the existing network can

Table 3: TOPOLOGY

Source IP addr	Dest IP addr	LQ	ILQ	ETX
192.168.0.100	192.168.0.101	0.498	0.596	3.37
192.168.0.100	192.168.0.102	1.000	0.898	1.11
192.168.0.100	192.168.0.103	1.000	1.000	1.00
192.168.0.101	192.168.0.100	0.200	0.400	12.50
192.168.0.101	192.168.0.102	0.498	0.298	6.74
192.168.0.101	192.168.0.103	0.498	0.400	5.02
192.168.0.103	192.168.0.100	1.000	1.000	1.00
192.168.0.103	192.168.0.101	0.592	0.596	2.83
192.168.0.103	192.168.0.102	1.000	0.898	1.11

Table.3. provide the complete information about all the types of routes possible in the existing network. LQ gives the

quality of link determined by source node whereas ILQ gives the quality of link determined by destination node. ETX = 1/ILQ*LQ. We want to obtain the minimum value of ETX.

Table 4: DIJKSTRA

192.168.0.100:1.11 (one-hop)
192.168.0.101:4.17 (one-hop)
192.168.0.103:1.11 (one-hop)

Table.4. gives the destination node and total value of ETX from source to destination. The right nodes used to be neighbor nodes but in our case due to the small network, all destinations are at one hop distance only.

VI. Conclusion and future work

In this paper, we have presented a study based comparison of ZRP AND OLSR routing protocol. We highlighted different aspects of these two techniques and presented a brief description of their applicability and operational details. We simulated a wireless network and successfully routed the packets in an Ad Hoc environment making use of Optimized link State Routing Protocol (OLSR) where each node acts as a router and makes use of Multi Point relay technique.

Our future work extends this study based comparison and proposed work in Section IV into a more intense simulation-based comparison.

VII. References

Periodicals:

[1] E.M.Belding-Royer and C.K.Toh., “A review of current routing protocols for ad-hoc mobile wireless networks,” IEEE Personal Communications Magazine, pages 46-55, April 1999.

[2] L.Zhou and Z. hass. “Securing ad hoc networks,” IEEE Network. 13(6):24-30, November/December 1999.

[3] Marc R. Pearlman and Zygmunt J. Hass, “Determining the optimal configuration for zone routing protocol,” Selected Areas in Communication, IEEE journal on August 1999, vol 17, No 8

[4] S.Murthy and J.J.Garcia-Lana_Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, pp. 183-197, October 1996.

Books:

[5] C. E. Perkins, “Ad Hoc Networking,” Addison-Wesley, 2000

[6] DAVID B. JOHNSON, DAVID A. MALTZ: “Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Thomasz Imielinski and Hank Korth (Editors) ,” Vol. 353, Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996.

Technical Reports:

[7] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, “A secure routing protocol for ad hoc networks” Technical Report 01-37, Computer Science Department, University of Massachusetts, August 2001.

Conference Proceedings:

[8] Shahan Yang and John S. Baras, “Modeling Vulnerabilities of Ad Hoc Routing Protocols,” ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03) October 31, 2003

[9] J.P. Hubaux, L. Buttyab, and S. Capkun., “The quest for security in mobile ad hoc networks,” In Proc. ACM MOBICOM, 2001

[10] Srdjan Capkun and Jean-Pierre Hubaux, “BISS: Building Secure Routing out of an Incomplete Set of Security Associations,” ACM Workshop on Wireless Security (WiSe 2003) September 19, 2003

[11] Charles E. Perkins and Pravin Bhagwat , “Highly Dynamic Distance Vector Routing for Mobile computers”’, ACM SIGCOMM Computer Communication Review,October 1994, vol 24, No 4, pp 234-244

[12] Rajendra V. Boppana and Satyadeva P Kondru, “An Adaptive Distance Vector Routing Algorithm for Mobile Ad Hoc Network”’, INFOCOM 2001 Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. vol 3, pp 1753-1762

[13] P. Jacquet, P. Muhlethaler, T. Clausen, A.Laouiti, A.Qayyum,L. Viennot “Optimized Link State Routing Protocol for Ad Hoc Networks,” Multi Topic Conference, 2001. IEEE INMIC March, 2001. pp 62-68

[14] Thomas Heide Clausen, Gitte Hansen, Lars Christensen, Gerd Behrman “The Optimized Link State Routing Protocol Evaluation Through Experiments And Simulation,” IEEE Symposium on Wireless Personal Mobile Communications, 2001

[15] Amir Qayyum, Laurent Viennot and Anis Laouiti , “Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks,” in System Sciences, Jan,2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference, pp 3866-3875

[16] Y-C Hu, A. Perrig, D. B. Johnson, “Ariadne : A secure On-Demand Routing Protocol for Ad Hoc Networks,” in proceedings of MOBICOM 2002.

[17] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Fourth IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. “Efficient Security Mechanisms for Routing Protocols,” Proceedings of the Tenth Annual Network and Distributed System Security Symposium (NDSS 2003), ISOC, San Diego, CA, February 2003.

[19] C. PERKINS, E.ROYER AND S. DAS “Ad hoc On-demand Distance Vector (AODV) Routing,” RFC 3561

[20] ZYGMUNT J. HAAS, MARC R. PEARLMAN, PRINCE SAMAR, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” Internet Draft”

[21] Y. Chu, A. Perrig, D. Johnson, “Ariadne - A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. ACM Conf. Mobile Computing and Networking (MobiCom), 2002.

Url:

[22] http://hipercom.inria.fr/OOLSR/

[23] http://www2.net.ie.niigata-u.ac.jp/olsr-e.php

[24] http://www.softpedia.com/get/Network-Tools/Network-Tools-Suites/OLSR-daemon.shtml

[25] GlomoSim http://pcl.cs.ucla.edu/projects/glomosim/obtaining_glomosim.html

VIII. Biographies

Akshai Aggarwal (M’1966, SM’1992) is working as Director, School of Computer Science, University of Windsor. He was Professor and Head of Department of Computer Science at Gujarat University for about 10 years. Before that he was Professor and Head, Department of EE at M.S.University of Baroda. He has been actively associated with the IEEE platform in India. He was Chairman of IEEE India Council for two years. He initiated IEEE activities in Gujarat by starting the first IEEE Student Branch at M.S.University of Baroda. Later he initiated the establishment of the Student Branch at Gujarat University. He was also the founder Chairman of IEEE Gujarat Section, the IEEE Computer Society Chapter and the IEEE Joint Chapter of Industry Applications, Industrial Electronics and Power Electronics. The Section conducted two International Conferences and one national Seminar during his Chairmanship. He graduated with a B.Sc.(EE) from Punjab Engg College and studied at MS University of Baroda for his Master’s and Doctoral work.

E-mail: akshaia@uwindsor.ca

Savita Gandhi (M' 2003 SM' 2005) is Professor & Head at the Department of Computer Science, Gujarat University and Joint Director, K.S. School of Business Management, Gujarat University. She is with Gujarat University for about 20 years. Before that she has worked with M.S. University of Baroda, Department of Mathematics for about 10 years. She has been actively associated with IEEE activities. To mention few : SPCTS 2003 & International Workshop and research seminar on Cluster Computing under the joint activities of Department of Computer Science and IEEE , Gujarat Section . She has also served as Student Chair, IEEE, Gujarat Section. She is M.Sc. (Mathematics), Ph.D (Mathematics) and A.A.S.I.(Associate Member of Actuarial Society of India by the virtue of having completed the "A" group examinations comprising six subjects conducted by Institute of Actuaries , London). She was awarded Gold Medal for standing first class first securing 93% marks in M.Sc. and several prizes at M.Sc. as well as B.Sc. Examinations for obtaining highest marks.
E-mail: drsavitagandhi@rollwala.org

Nirbhay Chaubey (S'2002, M'2004) is working as a Lecturer of Computer Science at Institute of Science and Technology for Advanced Studies and Research, Vallabh Vidyanagar, Gujarat, India. Currently, he is pursuing Ph.D in Computer Science at Department of Computer Science, Gujarat University, Ahmedabad, India. He has been involved in IEEE activities since 1994. His position held for IEEE Gujarat Section include Executive Secretary (1994-2005), Treasurer (2005-2006), Secretary and Treasurer (2007) and Treasurer for year 2008. He coordinated several IEEE activities in Gujarat. He has endorsed and nominated to form an IEEE Student Branch at ADIT Engineering College, GCET Engineering College and ISTAR Engineering College all three at Vallabh Vidyanagar, Gujarat, India. He graduated from Ranchi Unviersity, Ranchi, and Master in Computer Applications from Madurai Kamraj University, Madurai, India
E-mail: nirbhay@ieee.org