Routing Protocols in MANET

K. Maheshwari MCA., M.Phil.,
Department of Computer Science department,Wavoo wajeeha women's college, Kayalpatnam.
E-mail: mahi.msu@gmail.com

M.Sahaya Agnel Rigana MCA., M.E.,
Department of Computer Science department,Wavoo wajeeha women's college, Kayalpatnam.
E-mail: riganaa@gmail.com

ABSTRACT

MANET is a self organized and self configurable network where the mobile nodes move arbitrarily. The mobile nodes can receive and forward packets as a router. Routing is a critical issue in MANET. The objective of this paper is to compare the performance of adhoc routing protocols in MANET. There are several familiar routing protocols like Destination Sequenced Distance Vector (DSDV), Adhoc On-demand Distance Vector(AODV), Zone Routing Protocol(ZRP), etc… which have been proposed for providing communication among all the nodes in the network. This paper presents a performance comparison of three adhoc routing protocols such as Fisheye State Routing (FSR), Location Aided Routing(LAR1) and AODV with standard Dynamic Source Routing(DSR). The performance of the above three protocols are analyzed by three metrics: packet delivery ratio, average end-to-end delay and throughput using GloMoSim simulator. The experimental results show that LAR1 performs better than the other two methods.

Keywords- AODV, FSR, LAR1, Mobile Adhoc Network (MANET), Routing,

---

I. INTRODUCTION

Mobile ad-hoc network [S.Corson *et.al*,1999] is an autonomous system of mobile nodes connected by wireless links. Each node operates as an end system and a router for all other nodes in the network. In a mobile ad hoc network, nodes move arbitrarily, therefore the network may experiences rapid and unpredictable topology changes. Additionally, because nodes in a mobile adhoc network have limited transmission ranges, some nodes cannot communicate directly with each other. Hence, routing paths in mobile ad hoc networks potentially contain multiple hops. Mobile ad hoc networks have advantages such as rapid and ease of deployment, improved flexibility and reduced costs. Mobile adhoc networks are appropriate for mobile applications either in hostile environments where no infrastructure is available, or temporarily established mobile applications which are cost crucial. Typical application examples include a disaster recovery or a military operation. But in recent years, application domains of mobile ad hoc networks gain more and more importance in non-military public organizations and in commercial and industrial areas. The MANET working group (WG) within the Internet Engineering Task Force (IETF) works specifically on developing IP routing protocols topologies. To improve mobile routing and interface definition standards for use within the Internet protocol suite.

Many routing protocols (DSDV [C.E. Perkins et.al, 1994], WRP [S. Murthy et.al, 1996], OLSR [P. Jacquet et.al], FSR [Guangyu Pei et al, 2000], DSR [J. Broch et.al], AODV [C.E. Perkins et.al, 1999], TORA [V.D. Park et.al, 1997],CBRP [M. Jiang et.al],DREAM[S. Basagni]) proposed within the MANET working group of IETF, are designed to scale in networks of a few hundred nodes. In these, Proactive routing protocols provide fast response to topology changes by continuously monitoring topology changes and disseminating the related information as needed over the network. Reactive routing protocols operate on a need to have basis, and can, in principle, reduce the signaling overhead. However, the long setup time in route discovery and slow response to route changes can offset the benefits derived from on-demand signaling and lead to inferior performance.

AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements. Nevertheless we can still maintain most of the advantages of basic distance vector routing mechanisms [Charles E. Perkins et.al, 1999]. Fisheye State Routing (FSR) scales well in large network and it describes various security issues in FSR, which was discussed by [Guangyu Pei et.al, 2000]. Young-Bae Ko and Nitin H. Vaidya suggests an approach to utilize location information (for instance, obtained using the global positioning system) to improve performance of routing protocols for ad hoc networks. By using location information, Location-Aided Routing (LAR) protocols limit the search for a new route to a smaller "request zone" of the ad hoc network. This results in a significant reduction in the number of routing messages.

The paper is organized as follows. Section II presents three routing protocols in MANETS namely AODV, FSR and LAR. Section III presents the results and analysis of the above protocols based on throughput, delay and PDR by varying nodes and mobility using GloMoSim simulator. Section IV concludes this paper.

II ROUTING IN MANETS

2.1 AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

Ad hoc On-Demand Destination Vector, (AODV) is a distance vector routing protocol that is reactive [Charles Perkins and Elizabeth Royer,1999]. The reactive property of the routing protocol implies that it only requests a route when it needs one and does not require that the mobile nodes maintain routes to destinations that are not communicating.

2.1.1 FLOW CHART

The following figure summarizes the action of an AODV node when processing an incoming message.

2.*1.1.1 AODV Protocol - Control Packets*

AODV uses four types of routing messages. They are explained as follows:

- RREQ

If a node wants to communicate with other node but no route is available, the source node starts a route discovery by broadcasting a Route REQuest (RREQ) message in the network.

- RREP

If it is a destination node or an intermediate node has a valid route to the desired destination, it replies to a RREQ by unicasting a Route REPly (RREP) message back to the source node.

- RERR

If a path breaks, the intermediate node generates a Route ERRor (RERR) message to inform its end nodes of the occurred link break.

- HELLO

Each node broadcasts periodically a message with time to live (TTL) = 1, in order to maintain its neighbor list.

2.1.1.2 AODV Route Discovery

When a node needs to determine a route to a destination node, it floods the network with a Route Request (RREQ) message. The originating node broadcasts a RREQ message to its neighboring nodes, which broadcast the message to their neighbors, and so on. To prevent cycles, each node remembers recently forwarded route requests in a route request buffer. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count.

When a node receiving the request either knows of a “fresh enough” route to the destination, or is itself the destination, the node generates a Route Reply (RREP) message, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed though these nodes to the destination.

Notice that it is possible for the RREQ originator to receive a RREP message from more than one node. In this case, the RREQ originator will update its routing table with the most “recent” routing information; that is, it uses the route with the greatest destination sequence number.

2.1.1.3 The Route Request Buffer

When a node originates or forwards a route request message to its neighbors, the node will likely receive the same route request message back from its neighbors. To prevent nodes from resending the same RREQs (causing infinite cycles), each node maintains a route request buffer, which contains a list of recently broadcasted route requests.

2.1.1.4 Expanding Ring Search

In flooding whenever a node requests a route, it sends a message that passes through potentially every node in the network. When the network is small, this is not a major concern. However, when the network is large, this can be extremely wasteful, especially if the destination node is relatively close to the RREQ originator. Preferably, we would like to set the TTL value on the RREQ message to be just large enough so that the message reaches the destination, but no larger. However, it is difficult for a node to determine this optimal TTL without prior global knowledge of the network.

To solve this problem, an expanding ring search algorithm is used, which works as follows. When a node initiates a route request, it first broadcasts the RREQ message with a small TTL value (say, 1). If the originating node does not receive a RREP message within a certain period of time, it rebroadcasts the RREQ message with a larger TTL value (and also a new RREQ identifier to distinguish the new request from the old ones). The node continues to broadcast messages with increasing TTL and RREQ ID values until it receives a route reply.

If the TTL values in the route request have reached a certain threshold, and still no RREP messages have been received, then the destination is assumed to be unreachable, and the messages queued for this destination are thrown out.

2.1.1.5 Link Monitoring & Route Maintenance

Each node keeps track of a precursor list, and an outgoing list. A precursor list is a set of nodes that route through the given node. The outgoing list is the set of next-hops that this node routes through. In networks where all routes are bi-directional, these lists are essentially the same.

2.2 FISHEYE STATE ROUTING (FSR)

Fisheye State Routing Algorithm (FSR) is a proactive or table driven routing algorithm which has been developed by Wireless Adaptive Mobility Laboratory, University of California, Los Angeles[Guangyu Pei, Gerla,M, Tsu-WeiChen,2000]. FSR is based on the traditional link state routing algorithm. Each and every node collects the information about the topology of the network from the neighboring nodes and calculates the routing table. It then disseminates the information locally to the neighboring nodes. The frequency of exchanging the routing information with neighbors depends on the distance between the source and the destination.

2.2.1 FLOW CHART

Fig 1.2 describes the overall working of FSR protocol.

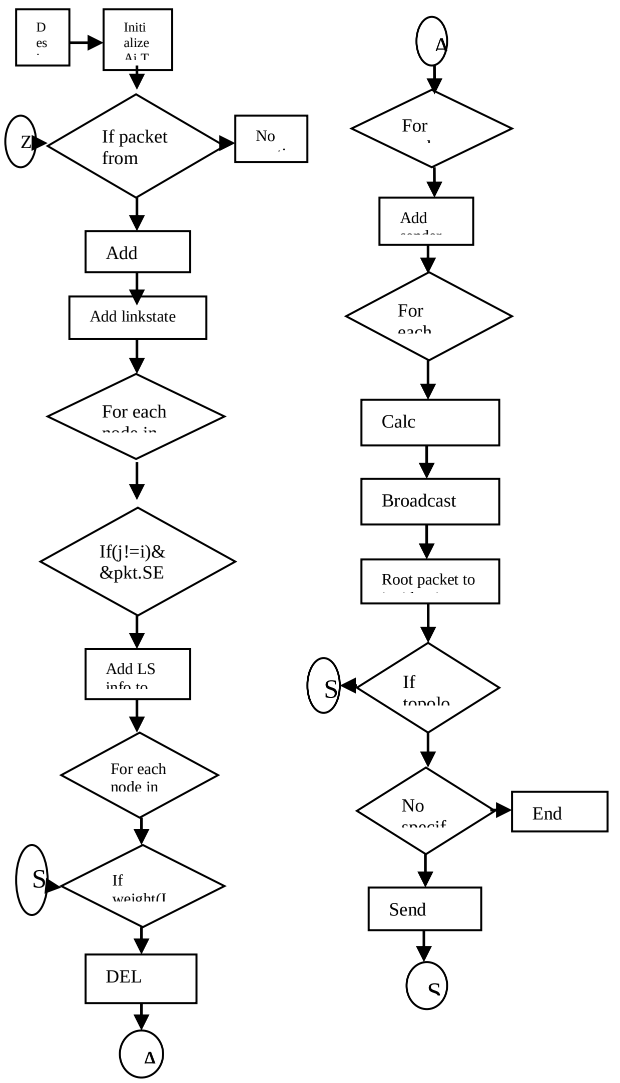


Figure 1.2 Flowchart for FSR

2.2.1.1 Representation of Network Topology in FSR

The network is represented as an undirected graph G= (V, E) where V=number of vertices or nodes in the network and E= number of edges or undirected links in the network. Each node has a unique identifier which represents a mobile host with a wireless communication device with transmission range R, and an infinite storage space. [5] A link between two nodes i and j is formed when the distance between i and j becomes less than R. The link (i, j) is moved if distance between i and j exceeds the range R. In FSR, for each node i, one list and three tables are maintained.

(i) A neighbor list Ai

(ii) A topology table TTi

(iii) A next hop table NEXTi

(iv) A distance table Di

Ai stores all the nodes those are neighbors to the node i. The topology table contains the most up to date information about the topology of the network from the link state message. The information in the topology table are required while calculating the routing table. The topology table has three fields; destination address, destination sequence number, link state list. Any destination j in TTi link state list has two parts TTi.LS(j) which denotes the link state information reported by node j and TTi.SEQ(j) indicates the time stamp at which j has generated the link state information. For each destination j, NEXTi(j) denotes the next hop to forward packets destined to j. Di(j) denotes the distance of the shortest path from i to j. A weight function can be used measure the distance of a link and is denoted by E-> Z0+ , which returns 1 if there is a direct link between two nodes , else, it returns ∞.

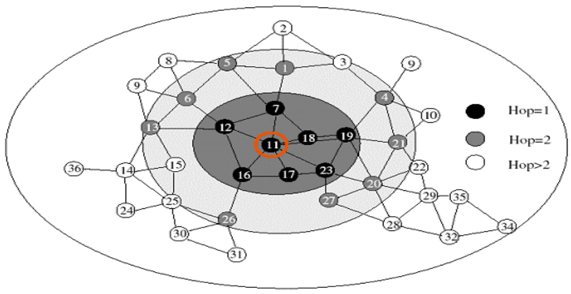


Figure1.2: FSR Protocol Description

FSR is based on the link state routing protocol but it differs in the way it disseminates routing update information or the link state information. In LS each node sends the link state packet by flooding whenever a topology change is detected by a node. But in FSR the nodes maintain a link state table and periodically exchange this table with the neighbors only. The selection of the frequency at which the LS table will be sent to the neighboring nodes depend on the distance between the two nodes. This is based on the fisheye technique. The eye of a fish captures with high details the pixels near the focal point of the fish eye. The detail decreases as the distance of the object increases from the focal point.

In FSR a full topology map is maintained at each node and shortest path is calculated using Dijikstra‟s algorithm. The scope of the fisheye is defined as a set of nodes that can be reached within a given number of hops and the scope has been shown in Figure -1.2 The number of levels and the size of the scope depends on the size of the network. GSR can be viewed as a special case of FSR with only one level and radius of the scope be ∞. FSR retains a routing entry for each destination; hence, it maintains low single packet transmission latency.

2.2.1.3 Link State Message Processing

When a node receives a link state message, it first checks its neighbor list Ai for the sender address. If the sender is a new one then it makes an entry in the neighbor's list. Otherwise, it will update the sequence number or the time stamp and the link state information about the sender in the list. Then the node processes the link state information contained the arrived message. While making its own link state packet for sending to the neighbors it copies the most update information from the link state messages to the topology table. In the incoming link state message if the sequence number is larger than the sequence number stored locally in the topology table about the node then only the message is taken into consideration for updating the old one stored in the table. Otherwise, if the sequence number shows an older number then that update message is discarded. Finally, if there are changes in the topology table, the routing table is updated.

2.2.1.4 Routing Table Calculation

The routing table of FSR provides the next hop information to forward the packets for the other destinations in the network. Whenever there are changes detected in the topology table of the node the routing table is updated. Based on the latest topology table the Dijikstra‟s algorithm is performed to find the shortest path from the current node to all the destinations those are in the topology table. The old routing table is replaced with the newly calculated routing table. The routing table has the following fields:

- Destination Address
- Next hop address
- Distance

In the FSR algorithm the weight or the link cost between two nodes has been taken as 1 and the weight function can be changed depending upon the requirement of functionality.

2.2.1.5 Data Packet Forwarding

FSR follows hop by hop data forwarding. The source node or any intermediate nodes retrieve the destination address from the data packet, and look at their routing tables. If the route is known, i.e., there is an entry for the destination, the data packet is sent to the next hop node. This procedure repeats until the packet finally reaches the destination. FSR does not provide any security feature for preventing a nodes misbehavior for not forwarding the data packet to the next node.

2.3 LOCATION AIDED ROUTING (LAR)

Location-Aided Routing (LAR)[F. A. Tobagi and L. Kleinrock,2000], as it makes use of location information to reduce routing overhead.

2.3.1 FLOW CHART

Fig 1.3 describes the working of LAR1 protocol.

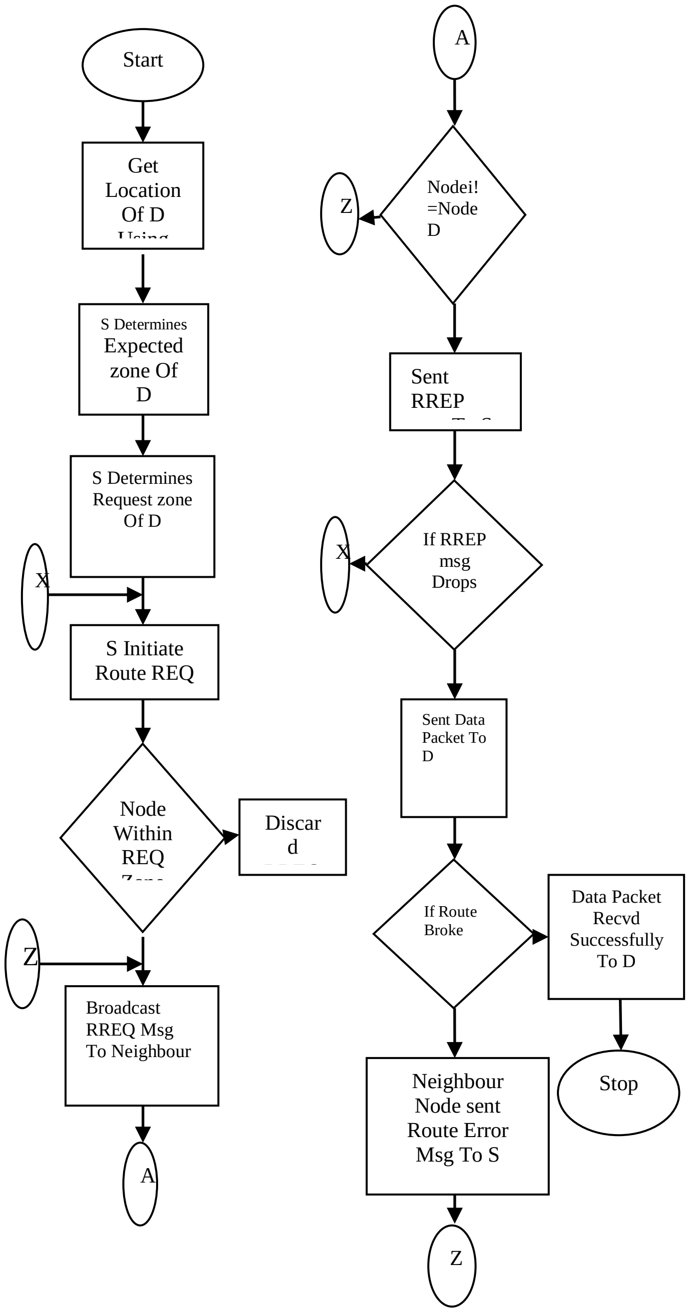


Figure 1.3 Flow chart for LAR1

2.3.1.1 Preliminaries

Location information

Location information used in the LAR protocol may be provided by the Global Positioning System (GPS). With the availability of GPS, it is possible for a mobile host to know its physical location.3 In reality, position information provided by GPS includes some amount of error, which is the difference between GPS-calculated coordinates and the real coordinates.

Expected zone and request zone

Expected zone: Consider a node S that needs to find a route to node D. Assume that node S knows that node D was at location L at time t0, and that the current time is t1. Then, the "expected zone" of node D, from the viewpoint of node S at time t1, is the region that node S expects to contain node D at time t1. Node S can determine the expected zone based on the knowledge that node D was at location L at time t0. For instance, if node S knows that node D travels with average speed v, then S may assume that the expected zone is the circular region of radius v(t1- t0), centered at location L (see figure 1.4(a)). If actual speed happens to be larger than the average, then the destination may actually be outside the expected zone at time t1. Thus, expected zone is only an estimate made by node S to determine a region that potentially contains D at time t1. In general, it is also possible to define v to be the maximum speed (instead of the average) or some other measure of the speed distribution.

If node S does not know a previous location of node D, then node S cannot reasonably determine the expected zone – in this case, the entire region that may potentially be occupied by the ad hoc network is assumed to be the expected zone. In this case, our algorithm reduces to the basic flooding algorithm. In general, having more information regarding mobility of a destination node, can result in a smaller expected zone. For instance, if S knows that destination D is moving north, then the circular expected zone in figure 1.4(a) can be reduced to a semi-circle, as in figure 1.4(b).

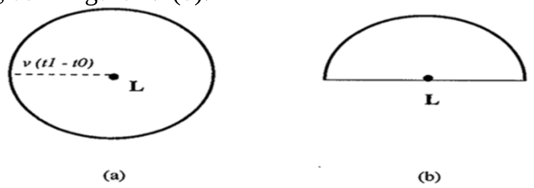


Figure 1.4: Examples of Expected Zone

Request zone. Again, consider node S that needs to determine a route to node D. The proposed LAR algorithms use flooding with one modification. Node S defines (implicitly or explicitly) a request zone for the route request. A node forwards a route request only if it belongs to the request zone. To increase the probability that the route request will reach node D, the request zone should include the expected zone (described above). Additionally, the request zone may also include other regions around the request zone. There are two reasons for this:

- When the expected zone does not include host S, a path from host S to host D must include hosts outside the expected zone. Therefore, additional region must be included in the request zone, so that S and D both belong to the request zone (for instance, as shown in figure 1.5(a)).
- If a route is not discovered within a suitable timeout period, our protocol allows S to initiate a new route discovery with an expanded request zone – in our simulations, the expanded zone includes the entire network space. In this event, however, the latency in determining the route to D will be longer (as more than one round of route request propagation will be needed). Note that the probability of finding a path (in the first attempt) can be increased by increasing the size of the initial request zone (for instance, see figure 1.5(c)). However, route discovery overhead also increases with the size of the request zone. Thus, there exists a trade-off between latency of route determination and the message overhead.

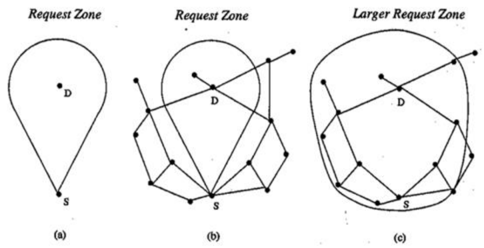


Figure 1.5: Request zone. An edge between two nodes means that they are neighbors.

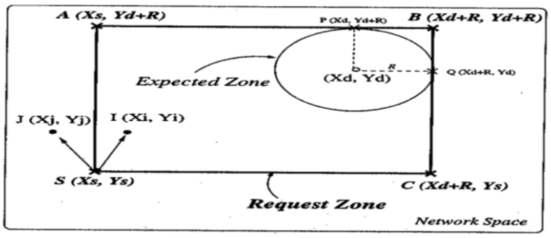
2.3.1.2 LAR scheme 1

LAR1 uses a request zone that is rectangular in shape (refer to figure 4.4). Assume that node S knows that node D was at location (Xd, Yd) at time t0. At time t1, node S initiates a new route discovery for destination D. The node S also knows the average speed v with which D can move. Using this, node S defines the expected zone at time t1 to be the circle of radius R = v(t1- t0) centered at location (Xd, Yd). (As stated before, instead of the average speed, v may be chosen to be the maximum speed or some other function of the speed distribution.)

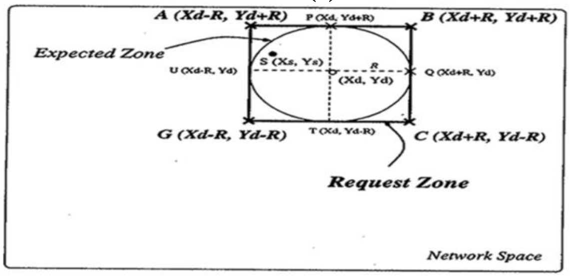
In LAR algorithm, the request zone to be the smallest rectangle that includes current location of S and the expected zone (the circular region defined above), such that the sides of the rectangle are parallel to the X and Y axes. In figure 1.6(a), the request zone is the rectangle whose corners are S, A, B and C, whereas in figure 1.6(b), the rectangle has corners at point A, B, C and G – note that, in this figure, current location of node S is denoted as (Xs, Ys).

The source node S can, thus, determine the four corners of the request zone. S includes their coordinates with the route request message transmitted when initiating route discovery. When a node receives a route request, it discards the request if the node is not within the rectangle specified by the four corners included in the route request. For instance, in figure 1.6(a), if node I receives the route request from another node, node I forwards the request to its neighbors, because I determines that it is within the rectangular request zone. However, when node J receives the route request, node J discards the request, as node J is not within the request zone (see figure 1.6(a)).

When node D receives the route request message, it replies by sending a route reply message (as in the flooding algorithm). However, in case of LAR, node D includes its current location and current time in the route reply message. When node S receives this route reply message (ending its route discovery), it records the location of node D. Node S can use this information to determine the request zone for a future route discovery. (It is also possible for D to include its current speed, or average speed over a recent time interval, with the route reply message. This information could be used in a future route discovery. In our simulations, we assume that all nodes know each other's average speed.)



(a)



(b)

Figure 1.6(a): Source node outside the expected zone
Figure 1.6(b): Source node within the expected zone

Size of the request zone.

Note that the size of the rectangular request zone above is proportional to (i) average speed of movement v, and (ii) time elapsed since the last known location of the destination was recorded. At low speeds, route discoveries occur after long intervals, because routes break less often (thus, t1- t0 is large).

III RESULTS AND ANALYSIS

3.1 Performance Metrics

Three key performance metrics are evaluated:

- *Packet delivery fraction*
  The ratio of the data packets delivered to the destination to those generated by the sources.
- *Average end-to-end delay of data packets*
  This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times.
- *Throughput*
  It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

  Throughput=∑Received packets/End Time

3.2 Experiments and Results

3.2.1 Simulation Environment

Simulations are configured for the performance evaluation of FSR, AODV, DSR, and LAR1 with the metrics like throughput, end to end elay and packet delivery ratio with the following parameters given in the following table 1.1

Table 1.1 General Experimental Setup Parameters

Experiment Parameter	Experiment Value
Simulation Time	300s
Terrain Dimension	1000mX1000m
No. of mobile nodes	10-100
Node Placement	Uniform, Random waypoint motion
Mobility Speed	100-500s
Mac/phy	Mac/802_11
Routing Protocol	FSR,LAR1,AODV,DSR

3.2.2 Performance Evaluation

The performance of the above discussed protocols with standard DSR are analyzed by the above listed parameters and the pictorial representation is shown in the following figures.

Pause time Vs Throughput

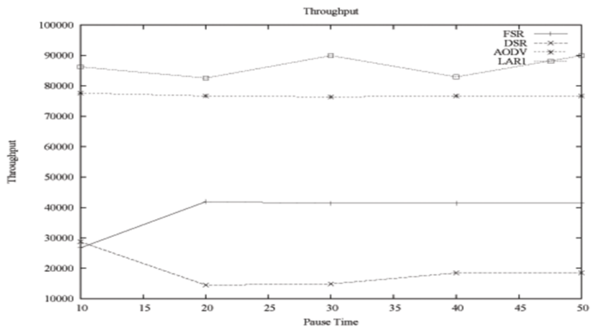


Figure 1.8 Pause Time(sec) Vs Throughput(kbps)

No of Nodes Vs Delay

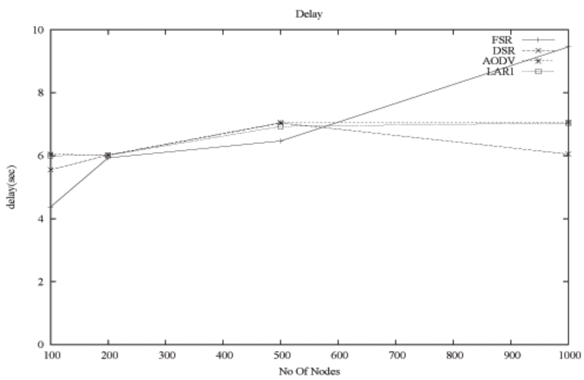


Figure 1.9 No of nodes Vs Delay(sec)

No Of Nodes Vs Packet Delivery Ratio

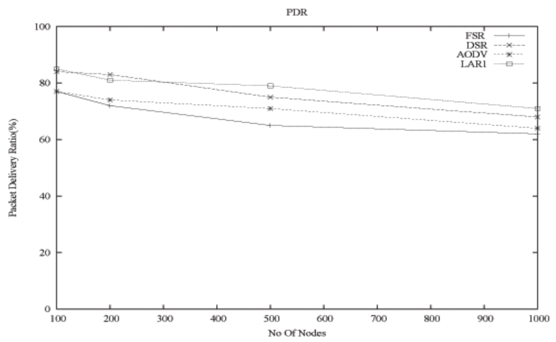


Figure 1.10 No of Nodes Vs Packet Delivery Ratio(%)

In Fig 1.8 we can observe the impact of mobility pause time on throughput. It shows that the throughput is getting constant while the pause time increasing beyond 20 seconds in case of LAR1,AODV and DSR. Fig 1.9 shows the graph between number of nodes and delay. This graph imply that other than FSR , all the other protocols having less delay and the delay is gradually increasing when number of nodes increases. Fig 1.10 shows the graph between Number of nodes and packet delivery ratio. This graph implies that LAR1 is having better packet delivering capability than AODV, DSR and FSR.

IV CONCLUSION AND FUTURE SCOPE

In this project AODV, FSR, LAR1 and DSR routing protocol has been studied for evaluating their performance. Performance evaluation metrics for these protocols were PDR, throughput and delay. The impact of mobility and scalability on the collision, PDR & delay were studied there. The comparison study between above three protocols shown that LAR1 performs better than all the others in case of throughput and delay. Next to LAR1, AODV has better performance in case of PDR, if mobility increases. For study the impact of scalability, the parameters were varying number of transmitted nodes & area of MANET. As the number of attackers increased, it caused more number of collisions. As the number of transmitted nodes was increased Packet Delivery Ratio of AODV, FSR, LAR1 were decreases constantly. Almost all protocol has less delay other than FSR, But FSR reduces overhead. In future, we can add security, scalability and reliability issues in LAR1.

IV REFERENCES

[1] R. Bagrodia, R. Meyer, M. Takai, Y. Chen, X. Zeng, J. Martin, and H.Y. Song, “PARSEC: A Parallel Simulation Environment for Complex Systems,” IEEE Computer, vol. 31, no. 10, Oct. 1998, pp.77-85.

[2] S. Basagni, I. Chlamtac, V.R. Syrotiuk and B.A. Woodward, A distance routing effect algorithm for mobility (DREAM), in: Proc. Of ACM/IEEE MOBICOM ’98 (1998).

[4] Charles Perkins and Elizabeth Royer. Ad hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop onMobile Computing Systems and Applications, pages 90–100, Feb 1999.

[5] S. Corson, S. Batsell and J. Macker, Architectural considerations for mobile mesh networking (Internet draft RFC, version 2), in: Mobile Ad-hoc Network (MANET) Working Group, IETF (1996).

[6] S.R. Das, C.E. Perkins and E. M. Royer, “Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks”, In Proceedingof IEEE INFOCOM 2000, Tel Aviv, Israel, Mar. 2000.

[7]Guangyu Pei, Gerla,M, Tsu-WeiChen, “Fisheye state routing: a routing scheme for ad hoc wireless networks” Communications, IEEE International Conference on Volume 1, Issue , Pages: 70-74 vol.1, 2000.

[8]P. Jacquet, P. Muhlenthaler, and A. Qayyum, “Optimized Link State Routing Protocol,” Internet Draft, draft-ietf-manet-olsr-*.txt,work in progress.

[9]M. Jiang, J. Li, and Y. -C. Tay, “Cluster Based Routing Protocol Functional Specification,” Internet Draft, draft-ietf-manet-cbrpspec*. txt, work in progress.

[10]S. Murthy and J.J. Garcia-Luna-Aveces, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and Applications J., special issue on routing in mobile communication networks, Oct. 1996.

[11]V.D. Park and M.S. Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” Proc. IEEE INFOCOM ’97, Apr. 1997.

[12] F. A. Tobagi and L. Kleinrock. Packet switching in radio channels: Part-II - the hidden terminal problem in carrier sense multiple-access models and the busy-tone solution. IEEE Young-Bae Ko and Nitin H. Vaidya “Location-Aided Routing (LAR) in mobile ad hoc networks” ,Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USATransactions in Communications, COM-23(12):1417–1433, 2000.