Simulation Based Performance Analysis of Ad hoc Routing Protocols in Various Moving Trajectories

Tanvi Malik,Gaurav Mittal, Monika Aggarwal
Department of ECE, B.G.IET, Sangrur, India

Abstract-Few characteristics of a Mobile Ad hoc Network, such as dynamic topology and shared wireless medium, pose various security challenges. This paper focuses on the performance investigation of reactive and proactive MANET routing protocols, namely, AODV and OLSR, under various the paths and trajectories. Network performance is evaluated in terms of end to end delay, retransmission attempts, network load and throughput, when a percentage of nodes misbehave. Simulation results show that under different parameters like end-to-end delay, proactive protocols perform well and under throughput parameter, performance of reactive protocols is robust.

Keywords-Ad Hoc, AODV, OLSR, Trajectories, Protocols

I. INTRODUCTION

Mobile Ad Hoc Network is simply known as MANET. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. In MANETs, communication between mobile nodes always requires routing over multi-hop paths. Nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. A mobile ad hoc network is formed by mobile hosts. Some of these mobile hosts are willing to forward packets for neighbors.

II. ROUTING PROTOCOLS

Routing is the act of moving information from a source to a destination in an internetwork. The main objective of ad hoc routing protocols is how to deliver data packets among nodes efficiently without predetermined topology or centralized control. Routing protocols use several metrics to calculate the best path for routing the packets to its destination. These metrics are a standard measurement that could be number of hops, which is used by the routing algorithm to determine the optimal path for the packet to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another [1]. Routing is mainly classified into static routing and dynamic routing [4]. Ad hoc wireless network routing protocols are further classified into three major categories based on the routing information update mechanism:

- **i.** Proactive or table driven routing protocols
- **ii.** Reactive or on-demand routing protocols

i. Reactive Routing Protocols

Reactive routing protocols, also known as on-demand routing protocols, a node creates a route in an on-demand fashion, and i.e. it computes a route only when needed. When a source wants to send packets to a destination, it invokes the route discovery mechanisms to find the path to the destination. Route discovery usually occurs by flooding a route request packet throughout the network. Route reply is sent back, if the destination itself or node with route to the destination is reached. There are various reactive routing protocols like AODV and OLSR

AODV: In AODV, the network is silent until a connection is needed. At that point the network node that needs a network connection broadcasts a request for new connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

ii. Proactive Routing Protocols

In proactive routing protocols, also known as table- driven routing protocols, each node maintains one or more tables that contain consistent and up-to-date routing information to every other node in the network. When the network topology changes, the nodes propagate update messages and the topology change information is distributed across the network. If the network topology changes too frequently, the cost of maintaining the network might be very high. Each node continuously evaluates routes to all reachable nodes. The overhead to maintain up-to-date network topology information is high [2]. There are many pro-active routing protocols:

OLSR: OLSR is a proactive link-state routing protocol, which uses Hello and Topology Control (TC) messages to discover and then disseminate link state information throughout

the mobile ad-hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths [3]. Being a proactive protocol, routes to all destinations within the network are known and maintained before use. Having the routes available within the standard routing table can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route. The routing overhead generated, while generally greater than that of a reactive protocol, does not increase with the number of routes being used. Default and network routes can be injected into the system by Host and Network Association (HNA) messages allowing for connection to the internet or other networks within the OLSR MANET cloud. Network routes are something reactive protocols do not currently execute well. Timeout values and validity information is contained within the messages conveying information allowing for differing timer values to be used at differing nodes.

III. Simulation Parameters and Results

The research is carried out using discrete event simulation environment software, known as OPNET (Optimized Network Engineering Tool) Modeler version 14.5. It is one of the most widely used commercial simulators based on Microsoft Windows platform.

The simulation focused on the performance of the routing protocols. Two types of network scenarios are designed: high density and low density networks. High density network consist of 80 nodes and low density network consist of 40 nodes.

For the comparison of protocols four different metrics have been chosen:

1. **Network Load (bits/sec):** Represents the total load (in bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network.
2. **Retransmission attempts (packets):** Total number of retransmission attempts by all WLAN MACs in the network, until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.
3. **Throughput (bits/sec):** Also known as packets delivery ratio or normalized throughput. It is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source.

Results of following parameters:

a) Network Load: Generally, the network load in AODV is lower than the OLSR due to the lower control load because OLSR has to publish the routing information to all the nodes in the network in the regular intervals of time. In AODV configured low density network (40 nodes), the network load is 43% lower than the OLSR in a well behaving network but when 50% of the nodes began to show selfish misbehavior, then the network load in AODV network is increased rapidly by 75% as shown in figure 1, while the change in the network load in OLSR network is negligible. Fig. 2 shows, the network load in a high density network (80 nodes). The increment of the network load in AODV configured network is increased by 88% while the results remain same for OLSR.

b) Retransmission Attempts*:* The average retransmission attempts of all wireless MACs in the network, either, the packet is discarded or successfully transmitted is decreased by 43% (Fig.3) in the case of AODV low density network (40 nodes), where, 50% of the nodes are misbehaving due to the selfishness attack because the 50% of the nodes are not generating, accepting and forwarding the packets in the network. In the case of OLSR low density network (40 nodes); retransmission attempts are decreased minutely by 3.8%. Fig. 4 shows that in high density AODV network (80 nodes) under selfishness attack, the retransmission attempts are decreased by 13.7%.

c) Throughput: In low density OLSR network (40 nodes), there is not any measurable change in the throughput (Fig. 5), where as in the case of AODV protocol network, the total throughput of network degrades by 67% because the packet drop is increased. To make things worse, when traffic load increases, congestion forces nodes to declare links failed although the links still exist. This leads to more routing overhead for repairing the broken links. Consequently, the control overhead grows very rapidly in AODV, when load increases. This growth is directly related to the throughput drop. In the high density networks (200 nodes) under denial of services attack, the throughput of an AODV network degrades by 52.3% and for OLSR network, this degradation is of 62.8% (Fig. 6).

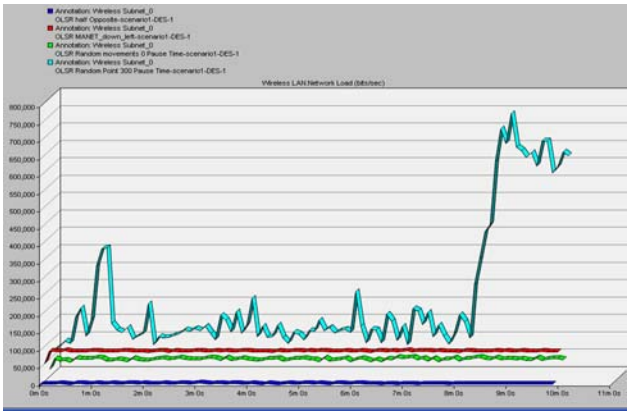

Fig 1 Network **Load in OLSR (bits/sec)**

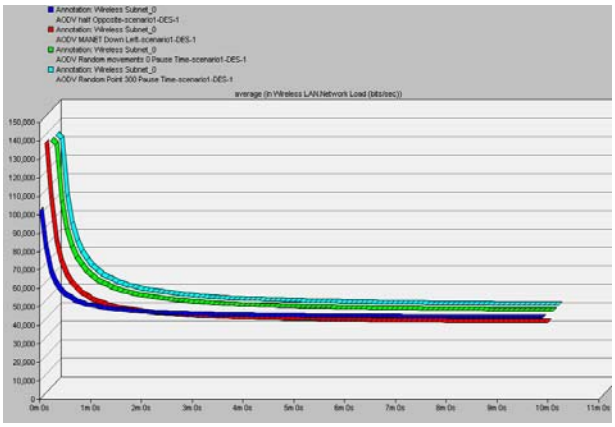

Fig 2 Network Load in AODV (bits/sec)

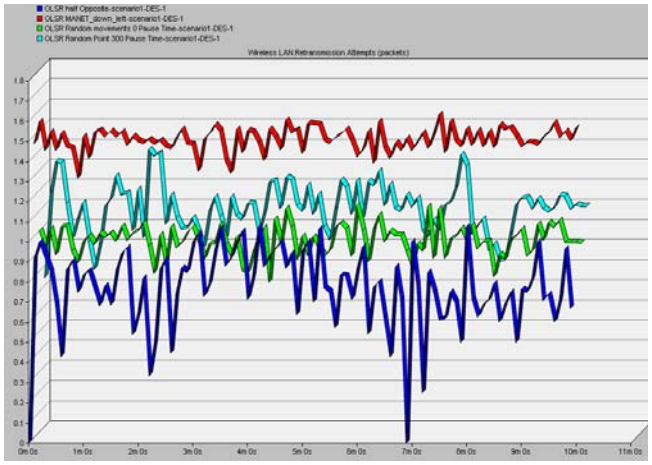

Fig 3 Retransmission Attempts in OLSR (Packets)

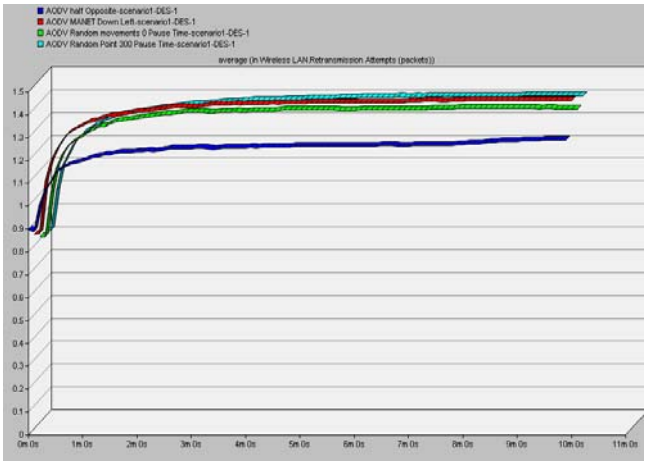

Fig 4 Retransmission Attempts in AODV (Packets)

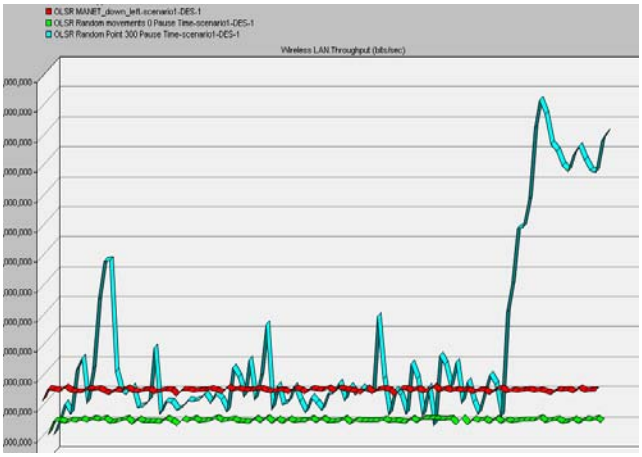

Fig 5Throughput in OLSR (bits/sec)

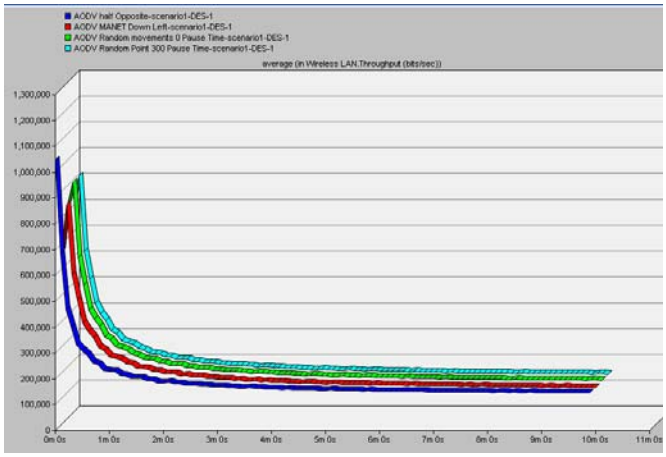

Fig .6 Throughput in AODV (bits/sec)

IV. CONCLUSION

From all the results it is concluded that proactive protocols performs better than the reactive protocols. If the performance of the network is evaluated on the basis of the throughput of the network because few authors consider the throughput as a main factor for the performance evaluation then reactive protocols outperforms the proactive protocols as the AODV did. But the overall performance of the network is better in OLSR then AODV, if all the performance evaluation metrics are considered. In future, the performance of various reactive and proactive protocols can be evaluated under various trajectories to make the results more justified.

V. REFERENCES

1. M.K. Jeya Kumar and R.S. Rajesh, “Performance Analysis of MANET Routing Protocols in Different Mobility Models.” In IJCSNS International Journal of Computer Science and Network Security.
2. N Vetrivelan and A V Reddy, “Performance Analysis of Three Routing Protocols for Varying MANET Size.” In Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008.
3. http://www.olsr.org/docs/report_html/node15.html.
4. Kuncha Sahadevaiah, “An Empirical Examination of Routing Protocols in Mobile Ad Hoc Networks” in Int. J. Communications, Network and System Sciences, 2010, 3, 511-522, June 2010.