International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

A Survey Paper on Mobility Model and Packet Size on PDR and Delay in MANET's

Mohd. Asif Khan[1]& Akhilesh Yadav[2]

Department of Computer Science and Engineering
Kashi Institute of Technology Varanasi U.P[1]
Kanpur Institute of Technology, Kanpur[2]
asifkhansoft@gmail.com[1]; akhil_jnp@rediffmail.com[2]

ABSTRACT

Ad-hoc Mobile/802.11 networks are those networks which has got no fixed topology due to the movement of end nodes. Each node within mobile adhoc network can act both host as well as router. For these mobile nodes to be properly functional and operational, routing protocol is required. And for this purpose, studies have being going on, which protocol is better. Little emphasis has been laid on network Performance indicator as which factors is most important for a specific Performance indicator. To the best of our knowledge no one has studied effect of different factors on network performance indicators like Packet delivery Ratio, Delay and Throughput and so on, as how much influence a particular factor or group of factors is having on network performance indicators itself Thus, in this work, effect of routing protocol, packet size and node mobility pause time have been evaluated against one of the most important network performance metric i.e. PDR and Delay.

Key words-
MANET; AODV; DSR; LAR1; PDR; Delay

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a self-configuring network of mobile devices and connected by non-wired links. In other words a MANET is a group of wireless mobile computers in which node moves in independent manner in any direction. The nature of MANETs brings a great challenge to system security. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may be multiple hops away from each other.

Networks can be classified into two forms (i) Infrastructure network and (ii) ad-hoc network. Infrastructure mobile network is that kind of network in which mobile devices depend on some fixed base station and that base station is controlled by other hand is that network, which is completely infrastructure less and does not depend on any base station. This network is a kind of temporary network and is used for emergency purposes like emergency services, military and so on. In this network, nodes move randomly and thus topology gets changed on regular intervals. Also, as mobile devises have certain power limitations there is limited communication range for these mobile nodes and due to this reason, sometimes nodes receive packets or send packets indirectly. Thus, this network is a kind of multiple hop network also due to different routing paths [1-5].

As nodes are always on the move, there are various mobility models available like random waypoint mobility model, group mobility model and many other mobility models which help us to depict a particular scenario. The purpose of mobility model is that, it gives us the idea during simulation as how can nodes move, for how much time these nodes can stop and wait, what will be the effect of movement by nodes on the performance of network and so on with varying speeds. Together mobility models and routing protocols help us in designing a particular scenario [6].

MANET is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range [4] of each other can directly communicate whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed and can work at

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

any place without the help of any infrastructure. The system may operate in isolation, or may have gateways to interface with a fixed network. This property makes MANET highly robust.

Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multihop routing. These mobile networks have following features that indicate more secure operation in the MANET.

1. The wireless link between the nodes is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited.

2. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link. Nodes continuously move into and out of the radio range. This gives rise to the change in routing information.

3. There is a bandwidth constraint in this wireless networks.

4. MANETS need energy - efficient operation because all the nodes depend on battery power which is highly limited.

Advantages: The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Disadvantages: Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

2. ROUTING PROTOCOLS FOR MANETS

Most widely used routing protocols for wireless ad hoc networks used in Glomosim simulator [12] available till today are Bellman-Ford, AODV, DSR, WRP, ZRP, FISHEYE and LAR1. All these protocols are constantly being improved by IETF. Since these protocols have different characteristics, the comparison of all performance differentials is not always possible. In this study we have considered three routing protocols AODV, DSR and LAR1.

A. Ad-hoc On Demand Distance Vector (AODV)

AODV [5, 6] shares DSR's on-demand characteristics in that it also discovers routes on an *as needed* basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops [5]. These sequence numbers are carried by all routing packets.

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is *expired* if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

The recent specification of AODV [6] includes an optimization technique to control the RREQ flood in

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

the route discovery process. It uses an *expanding ring search* initially to discover routes to an unknown destination. In the expanding ring search, increasingly larger neighborhoods are searched to find the destination. The search is controlled by the Time-To-Live (TTL) field in the IP header of the RREQ packets. If the route to a previously known destination is needed, the prior hop-wise distance is used to optimize the search. This enables computing the TTL value used in the RREQ packets dynamically, by taking into consideration the temporal locality of routes.

B. Dynamic Source Routing Protocol (DSR)

The key distinguishing feature of DSR [3, 4] is the use of *source routing*. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a *route cache*. The data packets carry the source route in the packet header.

When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a *route discovery* process to dynamically determine such a route. Route discovery works by flooding the network with *route request* (RREQ) packets. Each node receiving an RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a *route reply* (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed across the network. The RREP routes itself back to the source by traversing this path backward.1 The route carried back by the RREP packet is cached at the source for future use.

If any link on a source route is broken, the source node is notified using a *route error* (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source if this route is still needed.

DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the source route in a packet it forwards for possible future use. Several additional optimizations have been proposed and have been evaluated to be very effective by the authors of the protocol [7], as described in the following:

- *Salvaging*: An intermediate node can use an alternate route from its own cache when a data packet meets a failed link on its source route.
- *Gratuitous route repair*: A source node receiving an RERR packet piggybacks the RERR in the following RREQ. This helps clean up the caches of other nodes in the network that may have the failed link in one of the cached source routes.
- *Promiscuous listening*: When a node overhears a packet not addressed to it, it checks whether the packet could be routed via itself to gain a shorter route. If so, the node sends a *gratuitous* RREP to the source of the route with this new, better route. Aside from this, promiscuous listening helps a node to learn different routes without directly participating in the routing process.

C. Location-Aided Routing Protocol (LAR1)

The Location-Aided routing protocol (LAR) is a reactive (on-demand) routing protocol that uses the location information of the mobile nodes. Location information about nodes is obtained using Global Positioning System (GPS). LAR is advancement over Dynamic Source Routing (DSR) in context of route request packet flooding. In LAR, location information of the mobile nodes are used to flood a route request packet in a forwarding zone only called as request zone instead of the entire ad-hoc network. This request zone is determined by location information of the destination. Routing overhead in an ad-hoc network is reduced by the use of location information; this is one of the advantages of LAR. Complexity of protocol is nullified assuming accurately. A limitation of this protocol is every host requires a GPS device.
LAR defines two different types of request zones: LAR Scheme 1 (LAR1) and LAR Scheme 2 (LAR2). LAR1 [15] schemes use two zones: Expected zone and Request zone

Expected zone

Suppose, source node (S) knows that the destination node (D) was at some position P at time t0 and current time is t1. The expected zone of the node D

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

from the viewpoint of node S is the region that node S expects to have node D at time t1 based on the information that node D was at position P at time t0. The expected zone is only an estimation of node S for determining the possible positions of node D.

Request zone

Request zone for the route request packet forwarding is determined by the node S. An intermediate node forwards the route request packet only, if it belongs to request zone. The request zone includes expected zone and other surrounding zone around it. Routing mechanism of LAR1 is shown in figure 1. A rectangular shape request zone is the characteristic of LAR1. Once source knows that destination node was at a position (x0, y0) at time t0, expected zone at time t1 is defined by a circle with radius 'R = V(t1-t0)' centered at a position (x0, y0) where V is the average speed with which destination can move. Now a smallest rectangle defines the request zone that includes current source position and expected such that the sides of the rectangle are parallel to the X and Y axis. Source node S determines the four corners of the rectangular request zone and includes these coordinates in the route request packet when initiating the route discovery process. The neighboring nodes which are inside the request zone only forward the route request packet further while the outer nodes just drop the packets. Destination node sends backs a route reply packet with its current location, average speed and time as soon as it receives the route request packet. Node S uses this information for a route discovery process in future.

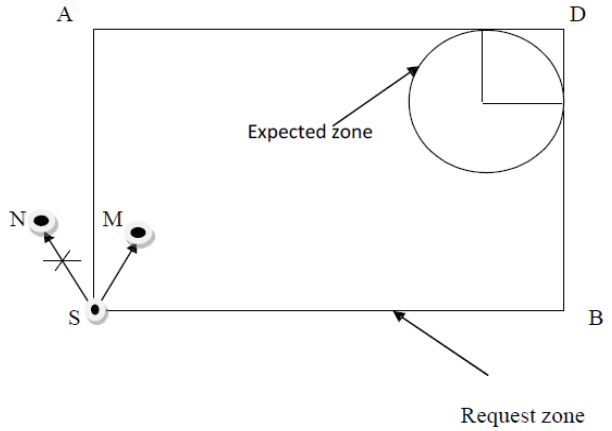

Figure 1: LAR1 routing mechanism

Location-Aided Routing (LAR1) routing protocol is an on-demand routing protocol which exploits location information. It is similar to Dynamic Source Routing (DSR) Routing protocol, but with the additional requirement of GPS information. In scheme 1 (implemented), the source defines a circular area in which the destination may be located, determined by the following information:

- The destination location known to the source
- The time instant when the destination was located at that position
- The average moving speed of the destination

The smallest rectangular area that includes this circle and the source is the request zone. This information is attached to a ROUTE REQUEST by the source and only nodes inside the request zone propagate the packet. If no ROUTE REPLY is received within the timeout period, the source retransmits a ROUTE REQUEST via pure flooding.

3. PERFORMANCE METRICES

These metrics are interesting because they can be used to point out what really happened during the simulation and provide valuable information about the routing protocol. In the following sections some metrics of this type are described.

A. Packet delivery ratio

The packet delivery ratio [11] presents the ratio between the number of packets sent from the application layer and the number of packets actually received at the destination nodes. It is desirable that a routing protocol keep this rate at a high level since efficient bandwidth utilization is important in wireless networks where available bandwidth is a limiting factor.

This is an important metric because it reveals the loss rate seen by the transport protocols and also characterizes the completeness and correctness of the routing protocol.

B. Routing overhead

Routing overhead is of course an interesting metric. In some way it reveals how bandwidth efficient the routing protocol is. The routing overhead metric simply shows how much of the bandwidth (which often is one of the limiting factors in a wireless system) that is consumed by the routing messages, i.e., the amount of bandwidth available to the data packets.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

An interesting observation is that for all protocols there is a theoretical limit where some properties of the scenario force the data rate down to zero because all the bandwidth is used for routing messages. The ideal case is naturally no overhead at all i.e., only data packets traverse the network. An ideal routing protocol can be implemented in a simulator but a routing protocol without routing messages is a contradiction and cannot be implemented in a real network.

The routing overhead [10] is typically much larger for a proactive protocol since it periodically floods the network with update messages. As mobility in the network increases reactive protocols will of course have to send more routing messages too. This is where the real strength or weaknesses of the routing protocol can be revealed.

In DSR another type of overhead presents itself even though it is easily overlooked in the previously described packet delivery ratio metric. DSR works by finding source routes to the destination on-demand. By storing information about all intermediate nodes in the packet header as the route discovery packet traverses the network it knows the full route once the route discovery packet returns. These source routes cause the packet headers to grow and hence produce more routing overhead. Considering this, the traditional metric, packets sent versus packets delivered, might give the impression that DSR is able to deliver more packets than other protocols. Looking at the ratio payload bytes sent versus payload bytes received instead could result in a different performance for DSR. This would be most obvious in a network with long routes (many hops).

C. End-to-end delay

The term end-to-end [3] is used to an average measure of performance between nodes in a network. It is the sources and the receivers that are involved. The end-to-end delay is therefore the total delay that a data packet experiences as it is traveling through a network. This delay is built up by several smaller delays in the network that adds together. These delays might be time spent in packet queues, forwarding delays, propagation delay (the time it takes for the packet to travel through the medium) and time needed to make retransmissions if a packet got lost etc.

Typically, in a packet based radio network without QoS (Quality of Service) [10] the delay could vary much depending on the routing protocol. One parameter that is critical is the time a packet is kept in a buffer before it is dropped if there is no route for its destination. This buffering time is controlled by a timer in each node. If this timer is set to a high value it could imply that packets are delayed in a network for this rather long period of time. A high value would probably decrease the number of dropped packets but it would also result in a somewhat higher average delay. Of course this is a question of what is important in a particular network, low delay or few dropped packets. It is a tradeoff that the system designer need to do, and as stated earlier, this will have an impact on the end-to-end delay.

D. End-to-end throughput

Since the available bandwidth in a network is fairly well known, it is interesting to see what the actual throughput achieved in a simulation is. If a good estimation of this value can be extracted it would be possible to see how efficient the routing protocol is. The higher the average throughput, the less routing overhead consuming the bandwidth.

E. Path optimality

Traditionally this measurement compares the optimal path usually defined as the shortest path between two nodes in the simulator at the sending moment with the length of the path that the packet actually travelled. If the average actual path length is close to the shortest path, the protocol is said to be good. However, it is hard to know what the actual optimal path is. Just settling with the shortest path does not address queuing and congestion in the network or high latency links.

4. SUMMARY

In this paper we have studied the routing protocols AODV, DSR and LAR1 over various numbers of nodes and various speeds. Here we study five performance metrics like Packet Delivery Ratio, Routing Overhead, End-to-End Delay, Throughput and Path Optimality. And the studied shows that the behavior of routing protocols varies as the no. of nodes, speed of nodes (Nodes Mobility Models) and packet sizes are changed. The performance of routing protocols varies with the above models.

For future work we can implement other routing protocols with the above mobility models and different models (scenario). And we can use different performance metrics.

5. REFERENCES

[1] Saqib Hakak, Suhiami. A. Latif et al. "Effect of Mobility Model and Packet size on Throughput in MANET's" published in 5th International Conference on Computer and Communication Engineering in IEEE (2014).

[2] Ashish Gupta, et al, "Performance Comparisons of Node Mobility Models on Routing Protocols on MANET" International Journal of Advanced Information Science and Technology (IJAIST) Vol.27, No.27, July 2014 ISSN: 2319:2682 with Impact Factor 3.564.

[3] Shekher Srivastava, et al, "Impact of Node Mobility of Routing Protocols in MANET" International Journal of Scientific & Engineering Research Volume 4, Issue 4, Aprail-2013 ISSN: 2229-5518 with Impact Factor 1.2.

[4] Toh, C.-K.: Adhoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall, Englewood Cliffs (2002).

[5] Yadav, N.S., Yadav, R.P.: Performance Comparison and Analysis of Table Driven & On Demand Routing Protocols for Mobile Adhoc Networks. International Journal of Information Technology 4(2), 101-109 (2007).

[6] Pizada, A.A., McDonald, et al.: Performance Comparison of Trust-Based Reactive Routing Protocols. IEEE Transaction on Mobile Computing 5(6), 695-710 (2006).

[7] Belding-Royer, E.Royer, : Routing approaches in mobile adhoc networks. In: Basagni, S.,Counti, M., Giordano, S. (eds.) Adhoc Networking, IEEE Press, Wiley (2003).

[8] Working Group IEEE 802.11, April 2008. [Online] Available: http://www.ieee802.org/11.,3.00pm 2-Feb-2014.

[9] Chakeres and C. Perkins, "Dynamic MANET On-Demand (DYMO) Routing" IETF Internet- Draft, draft-ietf-manet-dymo-17.txt, Mar. 2009.

[10] Paulus, Rajeev, et al "Performance Analysis of Various Adhoc Routing Protocols in MANET using Variation in Pause Time and Mobility Speed" International Journal of Computer Application 73 (2013).

[11] Gupta, S. Balaji, et al. "Performance Evaluation of MANET Routing Protocols under Varying Node Mobility" International Journal of Engineering & Technology (0975-4024) 5.3 (2013).

[12] GLOMOSIM Simulator, Retrieved 15 June, 2010, [Online], Available: http://www.GloMoSim.com.