A Study on Node Mobility Model and Packet Size on Routing Protocols in MANET's

Anita Yadav
College of Science and Engineering, Jhansi.

Harpal Singh Kushwaha
College of Science and Engineering, Jhansi

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, Throughput and Delay.

Index Terms – MANET, Bellman-Ford, DSR, WRP, PDR, Delay, Throughput.

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 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 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. The characteristics of these networks are summarized below:

- Autonomous and Infrastructure-less
- Dynamic Network Topology
- Self-organization and Self-administration
- No Centralized controller and Infrastructure
- Intrinsic Mutual Trust
- Device Heterogeneity
- Bandwidth-Constrained
- Energy-Constrained Operation
- Multi-hop Routing
- Network Scalability
- Nodes can be both host or router
- Frequent Routing updates
- Limited Physical Security

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.

It is also true that the solutions to the wired networks do not workable to mobile ad hoc networks domain. Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.

2. Due to lack of Trusted Third Party adds it is very difficult to deploy or implement security mechanisms.

3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.

4. Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both inside and outside attacks in MANET, in which insider attacks are more difficult to deal with.

5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

2. RELATED WORK

In one of the paper by Saqib Hakak, Suhiami. A. Latif et al (2014) title "Effect of Mobility Model and Packet size on Throughput in MANET's" published in 5th International Conference on Computer and Communication Engineering in IEEE. The authors have compared performance of two protocols- AODV and DYMO under pause time and speed variation and have concluded which protocol is better [1].

In one of the paper by Paulus, Rajeev, et al (2013), the author have compared performance of three protocols- AODV, DYMO and DSR under pause time variations and has concluded which protocol is better [8].

Again Paulus, Rajeev, et al (2013) in there another paper analyzed performance of three routing protocols DSR, OLSR and ZRP based on variation of packet transmission time and pause time and concluded which protocol are better [9].

Gupta, S. Balaji, et al (2013) in their paper evaluated the performance and compared three MANET routing protocols AODV, DSR and DSDV in different mobility conditions while varying pause time and node density. Three mobility models included were Random Waypoint, Random Walk and Random Direction [10].

From the above mentioned studies, we can concluded that although routing protocols has been compared from each other with respect to performance under different mobility models and pause time but how much important mobility model is for a specific Network performance indicator or how much important is Node mobility pause time or many other important factors like packet size, Number of nodes and so on is really a research challenge and has not been studied.

3. MOBILE AD HOC NETWORK ROUTING PROTOCOLS

Routing protocols for Mobile ad hoc networks can be broadly classified into three main categories:

3.1 Proactive (table driven) Routing Protocols

Each node in the network has routing table for the broadcast of the data packets and want to establish connection to other nodes in the network. These nodes record for all the presented destinations, number of hops required to arrive at each destination in the routing table [4, 5]. The routing entry is tagged with a sequence number which is created by the destination node. To retain the stability, each station broadcasts and modifies its routing table from time to time.

The proactive protocols are appropriate for less number of nodes in networks, as they need to update node entries for each and every node in the routing table of every node. It results more Routing overhead problem. There is consumption of more bandwidth in routing table.

3.2 Reactive (on-demand) Routing Protocols

In this protocol, a node initiates a route discovery process throughout the network, only when it wants to send packets to its destination. This process is completed once a route is determined or all possible permutations have been examined [6, 7, 8]. Once a route has been established, it is maintained by a route maintenance process until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A route search is needed for every unknown destination. Therefore, theoretically the communication overhead is reduced at expense of delay due to route search.

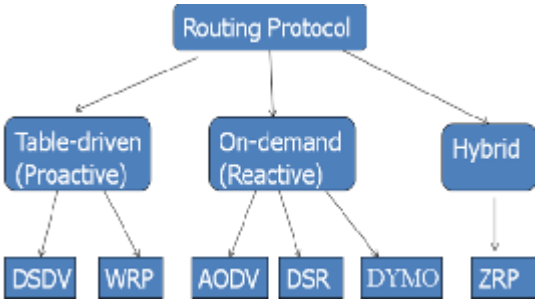

Figure 1. Categorization of Routing Protocols

3.3 Hybrid routing protocols

This protocol incorporates the merits of proactive as well as reactive routing protocols. Nodes are grouped into zones based on their geographical locations or distances from each other. Inside a single zone, routing is done using table-driven mechanisms while an on-demand routing is applied for routing beyond the zone boundaries [8, 9]. The routing table size and update packet size are reduced by including in them only art of the network (instead of the whole); thus, control overhead is reduced.

3.4 Bellman Ford

Bellman-Ford Routing Algorithm, also known as Ford-Fulkerson Algorithm, is used as a distance vector routing protocol. Routers that use this algorithm have to maintain the distance tables, which tell the distances and shortest path to sending packets to each node in the network. The information in the distance table is always updated by exchanging information with the neighboring nodes. Bellman Ford is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P. Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number. If a link presents the sequence numbers are even generally, otherwise an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

3.5 Dynamic Source Routing (DSR)

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. The destination node, on receiving a Route Request packet, responds by sending a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received. Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a Route Request packet. This Route Request is flooded throughout the network. Each node, upon receiving a Route Request packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's *time to live* (TTL) counter has not been exceeded. Each Route Request carries a sequence number generated by the source node and the path it has traversed.

3.6 Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) is a proactive unicast routing protocol for MANETs. WRP uses an enhanced version of the distance-vector routing protocol, which uses the Bellman-Ford algorithm to calculate paths. Because of the mobile nature of the nodes within the MANET, the protocol introduces mechanisms which reduce route loops and ensure reliable message exchanges.

The wireless routing protocol (WRP), similar to DSDV, inherits the properties of the distributed Bellman-Ford algorithm. To solve the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest path to every destination node and the penultimate hop node on the path to every destination node in the network. Since WRP, like DSDV, maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network. It differs from DSDV in table maintenance and in the update procedures. While DSDV maintains only one

topology table, WRP uses a set of tables to maintain more accurate information. The tables that are maintained by a node are the following: distance table (DT), routing table (RT), link cost table (LCT), and a message retransmission list (MRL).

4. PERFORMANCE PARAMETERS FOR COMPARISON

We will take four performance parameters for study on Bellman-Ford, DSR and WRP which are End-to End delay, Packet Delivery Ratio, Drop Ratio and Normalized Routing Load which are described as below:

4.1 End-to-End Delay

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. A low end-to-end delay is desired in any network.

The average time required for transmitting a data packet from source node IP layer to the destination IP layer, including transmission, propagation and queuing delay.

Average End-to-End Delay = Σ (Time when Packets enters in the Queue) - Σ (Time when the Packet is received)

4.2 Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network.

Packet Delivery Ratio = Σ (No. of Received Packets) / Σ (No. of Delivered Packets)

4.3 Throughput

Throughput is the number of packet that is passing through the channel in a particular unit of time. This performance metric show the total number of packets that have been successfully delivered from source node to destination node and it can be improved with increasing node density.

5. SUMMARY

In this paper we have studied about the various routing protocols like Bellman-ford, DSR and WRP and various performances metric like end to end delay, packet delivery ratio, and throughput.

In future work we can simulate the above mentioned routing protocols with the same performance metrics with varying the mobility model and varying the size of data packets and conclude their performance that how they behave with mobility model and packet sizes.

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] Toh, C.-K.: Adhoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall, Englewood Cliffs (2002).
[3] 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).
[4] Pizada, A.A., McDonald, et al.: Performance Comparison of Trust-Based Reactive Routing Protocols. IEEE Transaction on Mobile Computing 5(6), 695-710 (2006).
[5] Belding-Royer, E.Royer, : Routing approaches in mobile adhoc networks. In: Basagni, S.,Counti, M., Giordano, S. (eds.) Adhoc Networking, IEEE Press, Wiley (2003).
[6] Working Group IEEE 802.11, April 2008. [Online] Available: http://www.ieee802.org/11.,3.00pm 2-Feb-2014.
[7] Chakeres and C. Perkins, "Dynamic MANET On-Demand (DYMO) Routing" IETF Internet- Draft, draft-ietf-manet-dymo-17.txt, Mar. 2009.
[8] 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).
[9] Paulus, Rajeev, et al. "Comparative Study of DSR, OLSR and ZRP in MANET under Varying Pause Time and Packet Transmission Rate" International Journal of Computer Application 75 (2013).
[10] 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).