A Survey on Node Mobility Model and MAC Layer Protocols in MANET's

Alankrita Singh
B.Tech Student Department of CSE ITM GIDA, Gorakhpur

Apoorva Chhaparia
B.Tech Student Department of CSE ITM GIDA, Gorakhpur

Pranshikha Srivastava
B.Tech Student Department of CSE ITM GIDA, Gorakhpur

Ajay Kumar
Assistant Professor Department of CSE ITM GIDA, Gorakhpur

Abstract – with the advance of wireless communication technologies, small-size and high-performance computing and communication devices are increasingly used in daily life and computing. While the infrastructure cellular system is a traditional model for a mobile wireless network, here we focus on a network that does not rely on a fixed infrastructure and works in a shared wireless media. Such a network, called a *mobile ad hoc network* (MANET), is a self-organizing and self-configuring multihop wireless network, where the network structure changes dynamically due to member mobility. Nodes in this network model share the same random access wireless channel. Sometimes two or more nodes sending the information simultaneously results in collisions. Hence medium access controls (MAC protocols) are required for efficient transmission and avoiding collision. In this survey we study performance of various attributes like packet delivery ratio, end-to-end delay, drop ratio, throughput and routing overhead for three Routing protocols (AODV, DSR and WRP). In this paper we study two scenario of network i.e. mobility model and MAC layer protocol model.

Index Terms – MANET, CSMA, DSR, MACA, PDR, Delay, Throughput.

1. INTRODUCTION

Current mobile devices like Smart phones can handle many networking communication methods (e.g. cellular 2G/3G/4G, Wi-Fi, Bluetooth, NFC) whilst users are on the move. MANETs can be setup between Smart phones easily as no infrastructure is required. This is especially helpful in rural or disaster areas, where infrastructure-based networks (e.g. cellular) are not available. Rescue teams in disaster scenarios, remote scientific missions or ramblers, who want to communicate with each other, can also benefit from this type of networking. However, MANETs lack important secure network requirements like identity of all connected nodes and security of the data communication. This is because any device can join a MANET and MANET routing protocols have limited capabilities beyond establishing communication within the signal range.

To get over these limitations, devices normally rely on information collected about other nodes identity during previous communication or through the knowledge made available by others inside the network, to achieve "trust" in nodes joining the network. This simple "trust" model is not sufficient when the presences of many security threats that can forge or misuse this information are considered.

Moreover, protection for both:1) The route discovery process, and 2) All subsequent data transmissions should be kept in mind, too. In general, MANET routing protocols can be classified into two main types (i.e. proactive and reactive) based on the timing of route discovery. A third class (hybrid) combines algorithms of the other two types [1]. Proactive routing protocols, e.g. OLSR (Optimum Link State Routing), establish routes amongst present nodes in the vicinity prior to any data transmission. These routes are stored in tables and exchanged between nodes regularly, which allow establishing data communication routes quickly. A drawback of proactive protocols is the large overhead to maintain up-to-date routing information about the nodes, which makes proactive protocols not useful in larger networks of mobile devices. The required overhead would drain the resources and battery of these devices rapidly.

On the other extreme, reactive routing protocols establish connectivity on demand, whenever a node has data to transmit. The source node floods the air with route requests in an attempt to find a route to the destination. This flooding is propagated via other nodes until it reaches the desired destination. The destination then sends a traced route reply back to the source. As an example of such reactive protocols, AODV (Ad-Hoc ON Demand Distance Vector) introduces only little overhead but requires much longer establishing a route compared to proactive protocols. In addition, both protocol types do not provide any knowledge about the network structure beyond neighboring nodes. This is a major cause for delay and can introduce security vulnerabilities.

In MANET there are different routing protocols such as reactive, proactive, hybrid. All the reactive protocols such as AODV, DSR, etc. used to establish route between source and destination. Source node keeps on sending packets to the destination from all the nodes in the network until route establish between source and destination. In MANET every node acts as router which transfers information to other nodes.

- ***Characteristics:***

1. Dynamic Topology
2. No Centralized Controller
3. Power Limitation
4. Infrastructure less
5. Power Limitation

- ***Application of Manets:***

1. Used in Military applications
2. Used in Collaborative and Distributed Computing
3. Used in Emergency Operations

- ***Issues in Manets:***

1. Issue in Distributed operation
2. Issue in Hidden terminals
3. Issue in Access deferral

Carrier Sense Multiple Access (CSMA) CSMA [1] is standardized internationally in IEEE 802.11. It is contention based MAC layer protocol for wireless mobile ad-hoc network. This is packet based collision avoidance. It is probabilistic media access control protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium.

Multiple Access with Collision Avoidance (MACA) Multiple Accesses with Collision Avoidance (MACA) [1, 2] is a slotted media access control protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem.

This MACA protocol is not fully solve the hidden node and exposed terminal problem and nothing is done regarding receiver blocked problem.

- Contention Based Protocol
- Nodes are not guaranteed periodic access to the channel
- They cannot support real time traffic
- Three way handshaking
- RTS—CTS—Data packet exchange
- Binary Exponential back off Algorithm Sender initiated Protocol
- RTS—CTS carrier information about the duration of time for neighbor nodes.

Multiple access collision avoidance MAC layer protocol is three way handshaking techniques, known as RTS-CTS-DATA. There is no acknowledgment packet (ACK) in MACA scheme

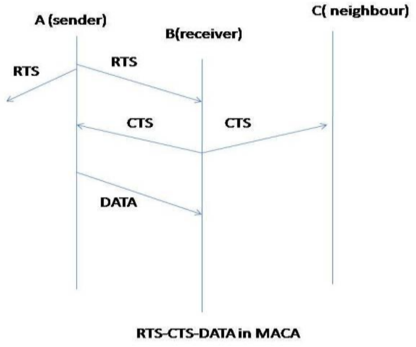

Figure 1. MACA Protocol

The basic idea of MACA is a wireless network node makes an announcement before it sends the data frame to inform other nodes to keep silent. When a node wants to transmit, it sends a signal called *Request-To-Send* (RTS) with the length of the data frame to send. If the receiver allows the transmission, it replies the sender a signal called *Clear-To- Send* (CTS) with the length of the frame that is about to receive. Meanwhile, a node that hears RTS should remain silent to avoid conflict with CTS; a node that hears CTS should keep silent until the data transmission is complete.

- When a node wants to transmit a data packet, it first transmits a RTS frame.
- The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.

If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.

2. 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 [2, 3]. 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.

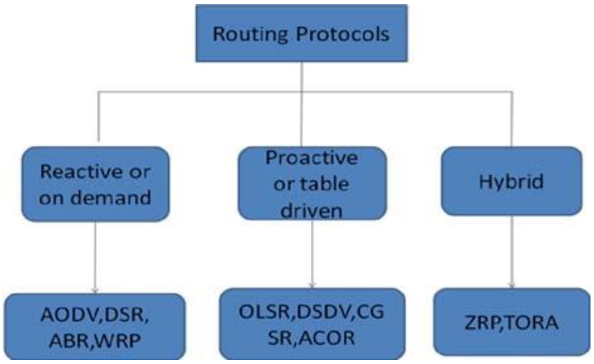

Figure 2. Categorization of Routing Protocols

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 [2]. 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 AODV

The Ad hoc On-Demand Distance Vector (AODV) [1] is an on-demand routing protocol that enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. This protocol performs Route Discovery using control messages route request (RREQ) and route reply (RREP), whenever node wishes to send packet to destination. To control network wide broadcast of RREQs, the source node uses an expanding ring search technique. The forward path sets up in intermediate nodes in its route table with a lifetime association using RREP. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. When either destination or intermediate node moves, a route error (RERR) is sent to the affected source nodes. When a source node receives the (RERR), it can reinitiate the route discovery if the route is still needed. Neighborhood information is obtained from broadcast Hello packet.

3.5 Dynamic Source Routing (DSR)

Dynamic source routing protocol (DSR) [4, 5] 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).

3. PERFORMANCE PARAMETERS FOR COMPARISON

We will take five performance parameters for study on Bellman-Ford, DSR and WRP which are End-to End delay, Packet Delivery Ratio, Throughput, 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.

4.4 Drop Ratio

Packet Drop rate is one of the indicators for network congestion. In wireless environment, due to the physical media and bandwidth limitations, the chance for packet dropping is increased. Therefore we choose it as one metric.

4.5 Normalized Routing Load (NRL)

Normalized Routing Load (NRL) is the ratio of control packets to data packets in the network. It gives a measure of the protocol routing overhead; i.e. how many control packets were required (for route discovery/maintenance) to successfully transport data packets to their destinations. It characterizes the protocol routing performance under congestion. NRL is determined as:

$$NRL = Pc / Pd$$

Where Pc is the total control packets sent and Pd is the total data packets sent.

4. SUMMARY

In this paper we have studied about the various routing protocols like AODV, DSR and WRP and various performances metric like end to end delay, packet delivery ratio, drop ratio, normalized routing load and throughput.

In future we can simulate the above mentioned routing protocols with the same performance metrics with varying the mobility model and MAC layer protocols and conclude their performance that how they behave with mobility model and packet sizes.

REFERENCES

[1] Ajay Kumar, Amit Kumar Kar et.al. , “Performance analysis of AODV, DSR & LAR1 Routing protocols for MANET" in ACEIT-16 Conference in Integral University in March 2016.

[2] 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).

[3] 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).

[4] 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).

[5] Uma Rathore Bhatt, Abhishek Dangarh et al , "Performance analysis of AODV & DSR Routing protocols for MANET" in 2014 Fourth International Conference on Communication Systems and Network Technologies 978-1-4799-3070-8/14 $31.00 © 2014 IEEE DOI 10.1109/CSNT.2014.

[6] Akshai Aggarwal, Savita Gandhi; “PERFORMANCE ANALYSIS OF AODV, DSDV AND DSR IN MANETS” International Journal of Distributed and Parallel Systems (IJDPS), November 2011, pp: 167-177.