COMPARISON OF DSR PROTOCOL IN MOBILE AD-HOC NETWORK SIMULATED WITH OPNET 14.5 BY VARYING INTERNODE DISTANCE

Puneet Mittal¹, Paramjeet Singh² and Shaveta Ram³

¹Dept. of Computer Engg. Govt. Poly. College, Bathinda, Punjab, India
²,³Dept. of Computer Science and Engg. GZS PTU Campus, Bathinda, Punjab, India

Abstract

In this paper, by changing their internodes distances, we compare the performance of Mobile ad hoc network (MANET). In this paper, we compare protocols DSR by using changing their internodes distances. We know that in ad hoc network, we communicate node by node by using interconnect network without any infrastructure. In ad hoc network each node works as a router. Each node having Wi-Fi capability for transfer the packets between each node or node by node. In case of mobile ad hoc network nodes can change the position. In mobile ad hoc network, the communication between nodes also can be done according to changing the topology of network.

Keywords— DSR, MANET, Protocol

1. INTRODUCTION

Ad hoc Network is may be fixed or dynamic (Mobile) ad hoc network. If the nodes are fixed in network, this type of network is called fixed ad hoc network (FANET). In this network data will be transmitted node by node which are fixed. If the node having mobility than this type of network is known as a mobile ad hoc network (MANET). We discuss Mobile ad hoc network because of sharing wireless medium they have capability to transmission of packets or data at for distances. Some times when nodes are nit in range of satellites or places where infrastructure is totally damaged this type of Ad hoc network is very useful for communication [1].

This paper is organised as follows. In sec. 2, we describe the routing protocol in MANET. Sec 3, gives the detail of Dynamic source routing (DSR) protocol in MANET. In sec 4, various parameters in traffic load. Sec 5 describe the simulation environment in this paper. In sec 6, we represent the results and discussion by using OPNET 14.5 Simulator. Conclusion is given in Sec 7.

2. ROUTING PROTOCOLS IN MANET

Routing protocols in MANET are divided into three categories: proactive, reactive and hybrid routing protocols.

2.1 PROACTIVE ROUTING:

Proactive protocols provide fast response to topology changes by continuously monitoring topology changes and disseminating the related information as needed over the network like OLSR, FSR, TBRP, FSLS Protocols.

2.2 REACTIVE ROUTING:

Reactive routing protocols such as Ad hoc in demand distance vector (AODV), find the route only when there is data to be transmitted as a result, generate low control traffic and routing overhead. Dynamic Source routing protocol (DSR), each data packet contains complete routing information to reach its dissemination and each node uses caching technology to maintain route information.
2.3 HIERARCHICAL ROUTING:
Hybrid protocol could be derived from the two previous ones, containing the advantages of both the protocols like HSR, ZRP, LANMAR and CGSR.

2.4 GEOGRAPHIC POSITION ROUTING:
Geographic routing is a routing principle that relies on geographic position information. It is proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. In this each node can determine its own location and that the source is aware of the location of the destination. With this information a message can be routed to the destination without knowledge of network topology or a prior route discovery like GEOCAST, DREAM, GPSR and LAR.

3. DYNAMIC SOURCE ROUTING (DSR)
DSR is also a reactive routing protocol. It uses the concept of source routing [2]. In source routing the sender knows all hop-by-hop routes to the destination. All the routes are stored in the route cache. When a node attempts to send a data packet to a destination it does not know the route. In DSR each node maintains a route cache with route entries which are continuously updated. The advantage of DSR is that no periodic routing packets are required. It is used to updates its route caches by finding new routes [3]. DSR has also the capability to handle unidirectional links. The sender of the packets selects and controls the route used for its own packets, which also supports features such as load balancing. All routes used are guaranteed to be free of loops as the sender can avoid duplicate hops in the selected routes [4]. The following sections introduce state machines that implement a simple DSR routing protocol without caching. There are basically 4 separate state machines to implement that each handles one of the following events [5]:

1. **SENDING DATA:** When a node wants to send data and data message is triggered as a send request then the next hop has be determined. A route request has to be broadcast to discover a route to the destination node. After receiving the route reply from the destination node the actual data message can be transmitted via the newly discovered.

![Figure 2: Flow Chart of Sending activity diagram](image)

2. **INCOMING ROUTE REQUEST MESSAGE:** When a route request message is received by a node, several tasks have to be done depending on the content of the received message. Firstly, it is checked whether the message was already processed earlier by this node. If yes, the request is simply discarded and no action is taken. If the route request is addressed to the receiving node, a route reply message has to be created and replied to the request’s sender. In all other cases the route request’s node list is extended by the own node ID and broadcasted to all neighboring nodes.

![Figure 3: Flow Chart of Route Request](image)
3. INCOMING ROUTE REPLY MESSAGE: In case a route reply message is received there are two cases: The receiving node is the destination of the message or it is an intermediate node on the route between sender and destination. If it is the destination node the data transmission that caused the route discovery can be accomplished. In case the route reply is received by an intermediate node, it is forwarded to the next node in the reply’s node list.

4. INCOMING DATA MESSAGE: If the data message is addressed to the receiving node (it is the last hop of the route) the payload can be handed to the upper layer to be processed by any application. The routing mechanism has finished. If not, the next hop is determined from the data message’s node list and the packet is forwarded to this node.

DSR contains 2 phases.

2.3.1 ROUTE DISCOVERY (FIND A PATH)

If sender node has in his route cache a route to the destination node, this route is immediately used. If not, the route discovery protocol is started:

Step 1: sender node sends a route request packet by flooding the network. Each route request packet contains: route record, initiator address, request ID

Step 2: if the route discovery is successful the initiating host receives a route reply packet.

Step 3: when any host receives a route request packet, it processes the request accounting to the following steps.

a) If <initiator address, request id> is found this host then discards the route request packet.

b) If this host’s address is already listed in the route record discard the route request packet.

c) If the target of the request matches this host’s address return a copy of this route in a route reply packet to the initiator.

d) Otherwise, append this host’s address to the route record and re-broadcast the request.

After getting the route reply the sender send the data to the destination.

i. ROUTE MAINTENANCE

In DSR every node is responsible for confirming that the next hop in the source route receives the packet. Also each packet is only forwarded once by a node (hop-by-hop routing). If a packet can’t be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop. Only if retransmission results in a failure, a Route Error message is sent to the initiator that can remove that source route from its route cache. So the initiator can check his route cache for another route to the target. If there is no route in the cache, a route request packet is broadcasted.
Step 1: if node C does not receive an acknowledgement form node D after some number of requests, it returns a Route Error to the initiator A.

Step 2: As soon as node receives the Route Error message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route.

Step 3: Otherwise the initiator A is starting the Route Discovery process again.

ROUTE CACHE
DSR uses route cache, in this route cache source node contains all the paths which are discovered in the route discovery process. Route cache contains necessary information regarding the network [6]. As the route cache store the discovered route, it can remove the unwanted route and overhead by eliminated the number of route request by considering the valid information and removing the invalid information. Route cache must be enough capable to store the all the paths which is in earlier route discovery process [7].

CACHE EXPIRY TIME
In the network when the nodes moves frequently, the connection between them are changes dynamically and cache hold this topology changes as the node interfaces with each other due to this it might be possible that a link in the cache which is not exist in the network. This information may create the many problems for sent packet. So we need a method which can delete the old entries from the cache after a certain interval of time called timeout, so chose this time out value is another critical issue. Here we have two method through which a timeout can be associated with each packet cache entry.

1. Static Timeout : When a link or path is added in the cache we add a predefined time T1 with this entry and when a reply comes through this link or path a different time T2 is associated in the remaining time.

2. Adaptive Timeout : This timeout associated with every link or path is dependent on the network condition.

4. VARIOUS PARAMETERS IN TRAFFIC LOADS

<table>
<thead>
<tr>
<th>SR. NO.</th>
<th>PARAMETERS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data dropped (Retry Threshold exceeded) (bits/Sec)</td>
<td>This statistic records the total amount of data that was received from the upper layer and then dropped by all WLAN nodes in the network due to repeatedly failed retransmission (i.e, exceeded the corresponding short retry or long retry threshold value).</td>
</tr>
<tr>
<td>2</td>
<td>Load (Bits/Sec)</td>
<td>This statistic records the total amount of data submitted by the upper layer for transmission by the WLAN layer on all the nodes in the network.</td>
</tr>
<tr>
<td>3</td>
<td>Media Access Delay (Sec)</td>
<td>This statistic records the medium access delay experienced by the packets submitted for transmission on all WLAN interfaces in the network. This value is computed as the interval from the time the packets was inserted into the transmission queue until the time when the packet was sent to the physical layer for the first time.</td>
</tr>
<tr>
<td>4</td>
<td>Network load (Bits/sec)</td>
<td>This statistic is computed on a per-BSS basic. It represented the amount of data from the higher layer that was received, accepted and queued for transmission by the entire WLAN BSS.</td>
</tr>
</tbody>
</table>

All these parameters help us to evaluate the best Routing area between 825km, 1000km and 1300km. All the parameters that have taken play a very vital role to judge or evaluate the performance of the wireless network.

5. SIMULATION ENVIROMENT
Several researchers have done the qualitative and quantitative analysis of ad hoc routing protocol area by means of different performance metrics. They have used different simulators for this purpose which is one of several tools provided from the OPNET Technologies suite. For undertake the experimental evaluation, the most recently available version, namely OPNET MODELER 14.5 has been adopted in our study OPNET is one of the most extensively used commercial simulators based on Microsoft Windows Platform, which incorporates most of the MANET routing parameters compared to other commercial simulators available [11]. The network entities used during the design of the network model are wireless server, application configuration, profile configuration, mobility configuration and workstations (nodes). Table 1 shows the various simulation parameters.
Table 2: Simulation parameters

<table>
<thead>
<tr>
<th>SIMULATION PARAMETER</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>OPNET MODELER 14.5</td>
</tr>
<tr>
<td>Area</td>
<td>825km, 1000km, 1300km</td>
</tr>
<tr>
<td>Network Size</td>
<td>20 nodes</td>
</tr>
<tr>
<td>Protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>FTP</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>900 (Sec)</td>
</tr>
<tr>
<td>Address Mode</td>
<td>IPv4</td>
</tr>
</tbody>
</table>

Figure 7: Environment Scenario of 20 Nodes in 825km

Figure 8: Environment Scenario of 20 Nodes in 1000km

Figure 9: Environment Scenario of 20 Nodes in 1300km

6. RESULTS AND DISCUSSION

FTP LOAD
6.1 Data dropped (retry threshold exceeded) (bits/sec)

![Image of graph showing data dropped over time]

**Figure 10:** Comparison of DSR Protocol for Data dropped (retry threshold exceeded) in FTP Load

In figure 15, X-axis denotes time in minutes and Y-axis is denotes data rate which is in bits/sec. It shows that the average peak value of Data dropped (retry threshold exceeded) is almost 6238.502924 bits/sec for 825km, 5110.081871 bits/sec for 1000km and 4973.660819 bits/sec for 1300km. After 15 minutes, it gradually drops to almost 3.259259259 bits/sec for 825km, 3.259259259 bits/sec for 1000km and 6.518518519 bits/sec for 1300km.

5.2 Load (bits/sec)

![Image of graph showing load over time]

**Figure 11:** Comparison of DSR Protocol for Load in FTP Load

In figure 5, X-axis denotes time which is in minutes and Y-axis denotes data rate which is in bits/sec. It shows that the average peak value of load is almost 6238.502924 bits/sec for 825km, 5110.081871 bits/sec for 1000km and 4973.660819 bits/sec for 1300km. After 15 minutes, it gradually drops as time progress and reaches to almost 3.259259259 bits/sec for 825km, 6.518518519 bits/sec for 1000km and 6.5185189 bits/sec for 1300km.

5.3 Media Access Delay (Sec)

![Image of graph showing media access delay over time]

**Figure 12:** Comparison of DSR Protocol for Media Access Delay in FTP Load

In figure 16, X-axis denotes time in minutes and Y-axis is denotes time in seconds. It shows that the average peak value of Media access delay is almost 0.146321001 seconds for 825km, 0.092589429 seconds for 1000km and 0.077394898 seconds for 1300km. After 15 minutes, it gradually drops and attains a constant value of approximately 0.013409719 seconds for 825km, 0.007971906 seconds for 1000km and 0.007152896 seconds for 1300km.
5.4 Network Load (bits/sec)

![Figure 13: Comparison of DSR Protocol for Network Load in FTP Load](image)

In figure 17, X-axis denotes time in minutes and Y-axis is denotes data rate which is in bits/sec. It shows that the average peak value of network load is almost 6238.502924 bits/sec for 825km, 5110.081871 bits/sec for 1000km and 4973.660819 bits/sec for 1300km. After 15 minutes, it gradually drops to almost 3.259259259 bits/sec for 825km, 6.518518519 bits/sec for 1000km and 6.518518519 bits/sec for 1300km.

Table 3 shows numeric values of various parameters taken into consideration for FTP load in DSR protocols. It gives the performance comparison of DSR protocols in terms of Data dropped (retry threshold exceeded), load, media access delay and network load for FTP load.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>DSR PROTOCOL</th>
<th>825 km</th>
<th>1000km</th>
<th>1300km</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data dropped (retry threshold exceeded)</td>
<td>6238.502924</td>
<td>5110.081871</td>
<td>4973.660819</td>
<td></td>
</tr>
<tr>
<td>Load (bits/sec)</td>
<td>6238.502924</td>
<td>5110.081871</td>
<td>4973.660819</td>
<td></td>
</tr>
<tr>
<td>Media Access Delay (Sec)</td>
<td>0.146321001</td>
<td>0.092589429</td>
<td>0.077394898</td>
<td></td>
</tr>
<tr>
<td>Network Load (bits/sec)</td>
<td>6238.502924</td>
<td>5110.081871</td>
<td>4973.660819</td>
<td></td>
</tr>
</tbody>
</table>

7. CONCLUSION

In this paper, we performed the comparison between 825km, 1000km and 1300km distance in DSR protocol with traffic load FTP in terms of Data dropped (retry threshold exceeded), Load, Media access delay and Network Load. The results are taken in tabular form as well as graphical form by using OPNET Simulator 14.5. The results show that which distance area is better for DSR protocol corresponding to FTP traffic load for some important parameters.

REFERENCES


