Comparison of DSR & MDSR Protocol

Vikas Jain,
Asst. Professor, Dept. of CSE,
CIST, Bhopal
Madhya Pradesh, INDIA.

Bhavana Gupta,
Asst. Professor, Dept. of CSE,
CIST, Bhopal
Madhya Pradesh, INDIA

Piyush Garg,
Asst. Professor, Dept. of CSE,
CIST, Bhopal
Madhya Pradesh, INDIA

***Abstract*— In the last decade with the advent of devices which support wireless network interfaces, the need of efficient protocols for the Network Layer and the Link Layer has increased. Networking Technologies use the services provided by the Link Layer to fulfill its task of Routing and Forwarding. Due to the dynamic nature of Mobile Ad Hoc Networks the legacy routing protocols of Wired Networks do not work efficiently in the Wireless Networks. There are three types of Protocols designed for the same, they are Proactive protocols (they are derived from the protocols designed for wired networks) and they maintain the routes to every nodes in the network by propagating route updates at fixed intervals, Reactive Protocols this class of protocol establish a route only when requested and Hybrid Protocol which combine both above mentioned approaches and try to bring out the best from the same.**

***Keywords*— Component; formatting; style; styling; insert (key words)**

1. INTRODUCTION

Wireless communication and network systems facilitate communication between computers using standard network without network cabling. Wireless Networks are classified into two types, viz, Access point networks and Ad-hoc networks. In access point networks, nodes use an access point or base station, which acts as a hub providing connectivity between two different nodes, wired and wireless LAN, a node and wireless LAN, etc., In Ad-hoc networks, direct communication between nodes is possible without any access points. Ad-hoc networks serve the issue of mobile nodes, due to its inherent properties such as self-organizing, self-healing, multi hopping, dynamic nature, etc., [3]. Because of its infrastructure less feature, ad hoc wireless networks provide the facility for the user to use the network services while continually moving.

The application scenario for the mobile Ad-hoc networks is emerging in recent years. Main issues of Ad hoc networks are routing, security, service location, energy consumption, etc. [4]. Routing the data using the intermediate nodes in Ad-hoc network becomes the major issue due to its dynamic characteristics.

Each move of the mobile nodes will change the topology of the network in the transmission route which sometime leads to the disconnection of link.

Since the communication is through radio waves, when there is a poor environment and the distance between the nodes is large, disconnection may occur. It is necessary that the routing protocols should also provide good route maintenance after the route discovery. The distinctive feature of these networks is that the network nodes need to collaborate with their peers in supporting the network functionality [5]. More probability exists for malicious or selfish nodes to disrupt or even deny the communication potentially of any node within the ad-hoc networking domain. Every node in the network is required to assist in the network establishment, network maintenance and network operation [6].Hence, establishing secured data transmission through secured routes becomes a predominant issue.

Generally, routing protocols are categorized as table driven and on demand. Table driven routing protocol maintain consistent and up to date routing information among the nodes in a routing table. On demand routing protocols discover a new route, when a route is required from the source to the destination node. It serves the user's issue in Ad hoc mobile networks [7]. Later, combinations of the features of above two types turn out hybrid routing protocol.

2. DYNAMIC SOURCE ROUTING PROTOCOL

The Dynamic Source Routing (DSR) is a reactive unicast routing protocol that utilizes source routing algorithm [8]. In source routing algorithm, each data packet contains complete routing information to reach its destination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt.

There are two major phases in DSR, the route discovery phase and the route maintenance phase. When a source node wants to send a packet, it initially consults its route cache. If the required route is available, the source node includes the routing information inside the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting route request packets. A route request packet contains addresses of both the source and the destination and a unique number to identify the request. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors. To limit the communication overhead of route request packets, a node processes route request packets that both it has not seen before and its

ISSN: 2278 – 7798

address is not presented in the route record field. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache.

After being created, either by the destination or an intermediate node, a route reply packet needs a route back to the source. There are three possibilities to get a backward route. The first one is that the node already has a route to the source. The second possibility is that the network has symmetric (bi-directional) links. The route reply packet is sent using the collected routing information in the route record field, but in a reverse order. In the last case, there exists asymmetric (uni-directional) links and a new route discovery procedure is initiated to the source. The discovered route is piggybacked in the route request packet [9, 10].

In DSR, when the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source.

DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance. DSR is only applicable to a relatively small amount of nodes, less than 100. Otherwise, managing the source routes to every node may become problematic.

3. MODIFIED DYNAMIC SOURCE ROUTING PROTOCOL

There are cases when the network size is big and there is unnecessary flooding in the network. The goal of the Modification is to limit the flooding. Suppose we have a scenario where we are using DSR and we usually communicate with nodes that are usually in a particular radius (radius is measured in hop count). Now whenever we try to establish a route between source and the destination there is unnecessary flooding of the network with Route Request. So instead of doing this we first try to find if the node is in the pre-defined radius. If we are able to establish the route than we have effectively reduced the number of forwarded packets and thus effectively decreased the overhead. If we are not able to find the route than we flood the whole network with the RREQ. The radius has to be defined keeping in mind the type of communication between the nodes i.e. The frequency at which a node communicates with a node in respect to the number of hops it takes to reach the destination node from the sender sender. Also we have to keep in mind that we are using 802.11 MAC, so the number of hops to reach a node might be less but it is possible that the route we get is of more length because of the flooding nature of the protocol and the inability of 802.11 to solve the hidden terminal problem.

So first we have to identify the First Request Radius which can be on basis of previous knowledge of the network or on the basis of heuristics done on the data communication pattern of the network. For analysis purpose we have taken the value to be 5 in this report.

4. SIMULATION AND ANALYSIS

We have done the simulation using network simulator tool NS-2. In this we have created the scenario based on different no. of nodes and accordingly we have arranged the nodes in linear and grid form. We have used the existing DSR routing protocol for the simulation and analysis of existing Dynamic source routing protocol. For modified DSR, we have create an agent in which first destination is searched within the predefined radius and if the destination is not available inside the circle then it broadcast to other neighboring nodes.

The fig-1 represents the graph where the network topology is linear. On X Axis is the hop count of the RREQ and on the Y Axis the time taken between the transmission of RREQ and RREP.

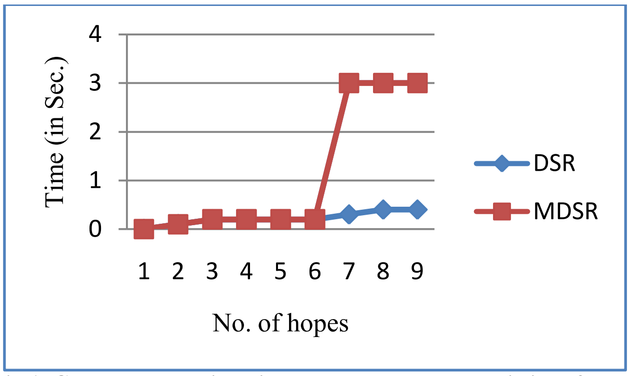

Fig-1: Graph Representing Time taken Between Transmission of RREQ and RREP

We can see the time taken by both the protocols in finding the destination till 5 hops is same but in case of MDSR it increases after the 5th hop. This suggests that the time for finding a route in case of MDSR is more for all those nodes which are not in the First Request Radius, here in simulation the first Request Radius is 5.

The fig-2 represents the graph where the network topology is grid. On X Axis is the time taken between the transmission of RREQ and RREP and on Y Axis is the number of nodes in the grid topology.

Fig-2 represents the graph between time taken to send the RREQ and RREP. We have observed as the number of nodes goes up, the average time to find the node goes up but the time taken by MDSR is less than the DSR. This

ISSN: 2278 – 7798

happens because in MDSR the nodes lie inside the First Request Radius in case of 4 x 4 and 5 x 5 grids.

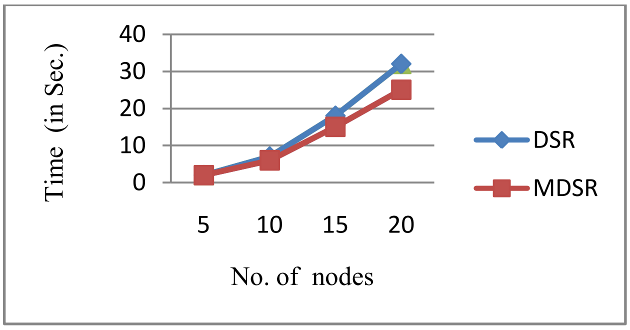

Fig: 2 Time taken between Sending RREQ and getting RREP

The given below graph represents the graph where the network topology is grid. On X Axis represents the no. of nodes and Y Axis represents the no. of packets forwarded.

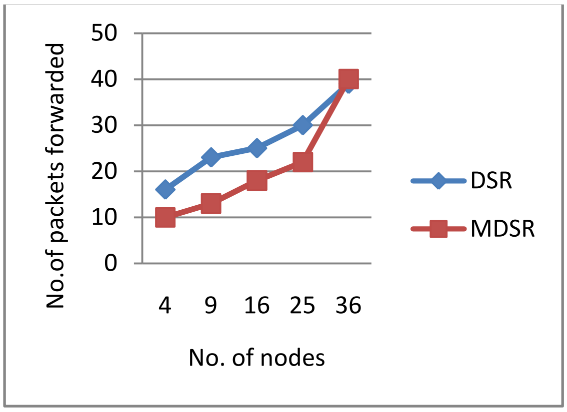

Fig 3: Graph representing the number of nodes vs the forwarded packets

As the number of nodes go up in grid topology the average number of packets that need to be forwarded decreases in MDSR in comparison to DSR. This happens because of restricted flooding in case of MDSR and the reason for the same number of packets in case of 3x3 and 2x2 grid is that all the nodes in this case lie inside the First Request Radius.

Fig 4 represents the graphs which give a comparison between the Average Number of Packets Forwarded to find a route vs probability of finding destination nodes.

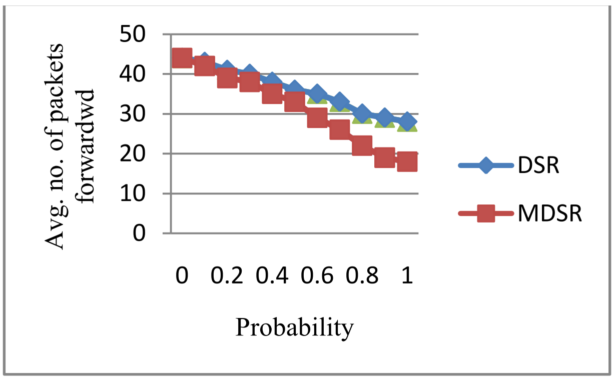

Fig 4: Avg. No. of Forwarded Packets vs Probability

The probability of finding the node inside the First Request Radius increase in case of MDSR so it requires less no. of packets to forward. We can see the decrease in the number of Packets forwarded in both the case but the decrease is much more in case of MDSR because of the restricted flooding approach we have taken in case of MDSR.

5. CONCLUSION AND FUTURE WORK

Here we can conclude by the simulations we have done that the performance of MDSR should increase in case when the network diameter is high and we would with high probability communicate with the nodes located in the certain hop radius of the network. Obviously there will be a tradeoff between the time taken to find the route and the number of packets forwarded by other nodes.

There is a need of more simulations for different kinds of topologies to test the Modified DSR. Also mobility can be a factor which can affect the performance of the modified DSR.

The protocol can be modified further such that it sends the route request first to a certain radius, if it does not find the destination it can increase the hop count in an additive fashion i.e. If it does not find the destination in a 5 hop radius then it will send another request in 8 hop radius and then in 11 hop radius and so on, the additive factor should be calculated on the basis of previous behavior of the network, mobility and other parameters.

REFERENCES

[1] T. R. Andel and A. Yasinac, "On the Credibility of MANET Simulations," IEEE Comp., vol. 39, issue 7, July 2006, pp. 48–54.

[2] I. Chlamtac, M. Conti, and J. Liu, "Mobile Ad Hoc Net-working: Imperatives and Challenges," Ad Hoc Net-works J., vol. 1, no. 1, Jan.–Mar., 2003.

[3] S. R. Das, R. Castaneda, and J. Yan. "Simulation-based Performance Evaluation of Routing Protocols for Mobile Ad hoc Networks", ACM/Baltzer Mobile Networks and Applications (MONET), 5(3): 179–189, 2000.

[4] Chakrabarthi S., Mishra A., "QoS issues in ad hoc wireless networks", communications magzine, IEEE, volume 39, issue 2, Feb 2001, pp.142-148.

[5] Elizabath.M.Royer and Chai-Keong Toh,"A review of current routing protocols for AdHoc mobile networks", IEEE personal communications, Volume 6, April 1999, pp-46 –55.

[6] G. ACS, L. Buttyan, I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[7] Huang R., Zhuang Y., Cao Q., "Simulation and Analysis of Protocols in Ad Hoc Network", 2009 International Conference on Electronic Computer Technology © 2009 IEEE.

[8] M. Weeks and G. Altun, "Efficient, Secure, Dynamic Source Routing for Ad-hoc Networks," Journal of Network and Systems Management, Vol.14, No. 4, pp. 559- 581, Dec. 2006.

ISSN: 2278 – 7798

[9] D. Johnson, D. Maltz, J. Jetcheva, “The dynamic source routing protocol for mobile ad hoc networks”, InternetDraft, draft-ietf-manet-dsr-07.txt, 2002.

[10] Broch J., Maltz D. A., Johnson D. B., Hu Y. C., and Jetcheva J., “A performance comparison of multi-hop wireless ad hoc network routing protocols,” ,ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM’98), October 1998, pp. 85–97.

VIKAS JAIN presently working in Corporate Institute of Science and Technology, Bhopal, as a Assistant Professor. He Secured M. Tech. (Hons) in CSE from DA-IICT, Gandhinagar, Gujrat. He Secured B.E in CSE from LNCT Bhopal, INDIA. E.mail: vikasjain.cse@gmail.com. His research interest includes Mobile adhoc Network, Network security.

BHAVANA GUPTA presently working in Corporate Institute of Science and Technology, Bhopal, as a Assistant Professor. She Secured M. Tech. (Hons) in CSE from Samrat Ashok Technological Institute Vidisha M.Pin 2010. She Secured B.E (Hons) in CSE from MITS Gwalior in 2001, SATI Vidisha, India. Tel:+91-9584559227 E.mail: bhavana_nishi@yahoo.co.in. Research Interest includes Mobile adhoc Network, Network security, Image Processing.

PIYUSH GARG currently working as a Asst. Professor in Department of CSE in Corporate Institute of Science and Technology, Bhopal, INDIA, He has completed his MTech in CSE from MANIT with Hons. He has done his BE in CSE from BIST, Bhopal, INDIA, E.mail: piyushgarg1985@yahoo.com. His research interest includes Mobile adhoc Network, Network security, Image Processing.

ISSN: 2278 – 7798