Routing Protocols in Mobile Adhoc Network (MANET)

Surendra H. Raut
M.Tech.-II
SGGS I E & T, Nanded

Hemant P. Ambulgekar
Assistant Professor
SGGS I E & T, Nanded

Abstract

Mobile Ad Hoc Network (MANET) allows portable devices to establish communication independent of a central infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols for mobile ad hoc networks are DSR, AODV and DSDV. Efficient routing protocols will make MANET reliable. Mainly protocols are of three kind i.e. proactive, reactive and hybrid. But, we will discuss proactive and reactive protocols. This paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The objective is to make observation about the working and performance metrics of these protocols. This paper presents the survey of routing protocols in MANET.

Keywords: *AODV, DSDV, DSR and MANET*

1. Introduction

In an ad hoc network [1], mobile nodes communicate with each other using multihop wireless links without infrastructure. Each node in the network also acts as a router, forwarding data packets for other nodes. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between two communicating nodes. In MANET nodes moves randomly, therefore the network may experience sudden and unpredictably change in topology. Nodes in MANET normally have limited transmission ranges, therefore some nodes cannot communicate directly to other nodes and those are beyond the limit of range of mobile node. So many protocols have been proposed for MANETs for achieving the efficient routing. Every protocol uses a new searching methodology for new route or modifying a known route, when hosts move. Energy consumption in MANET is very critical issue. Because, mobile devices have limited battery power and processing power. In MANET routing protocols can be divided into three categories: proactive routing protocols/table driven routing protocols, reactive routing protocols/demand routing protocols and hybrid routing protocols. Proactive routing protocols, consistent and up-to-date routing information to all nodes are maintained at each node. Reactive routing protocols, the routes are created, when required, when source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination.

2. Issues in MANET

If there are only two nodes that want to communicate with each other and are located very closely to each other, then no specific routing protocols or routing decisions are necessary. On the other hand, if there are a number of mobile hosts wishing to communicate, then the routing protocols come into play because in this case, some critical decisions have to be made such as which is the optimal route from the source to the destination which is very important because often, the mobile nodes operate on some kind of battery power. Thus it becomes necessary to transfer the data with the minimal delay so as to waste less power. There may also be some kind of compression involved which could be provided by the protocol so as to waste less bandwidth. In addition to this, Quality of Service support is also needed so that the least packet drop can be obtained. The other factors which need to be considered while choosing a protocol for MANET [1] are as follows:

2.1. Multicasting

This is the ability to send packets to multiple nodes at once. This is similar to broadcasting except the fact that the broadcasting is done to all the nodes in the network. This is important as it takes less time to transfer data to multiple nodes.

2.2. Loop Free

A path taken by a packet never transits the same intermediate node twice before it arrives at the destination. To improve the overall, we want the routing protocol to guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.

2.3. Multiple routes

If one route gets broken due to some disaster, then the data could be sent through some other route. Thus the protocol should allow creating multiple routes.

2.4. Distributed Operation

The protocol should of course be distributed. It should not be dependent on a centralized node.

3. Routing protocols

A routing protocol [2] is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. Many protocols have been suggested keeping applications and type of network in view. Basically, routing protocols can be broadly classified into three types as Table Driven Protocols or Proactive Protocols, On-Demand Protocols or Reactive Protocols and hybrid routing protocols. But, here we are discussing only proactive and reactive protocols.

3.1. Table Driven or Proactive Protocols

In Table Driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes keep on updating these tables to maintain latest view of the network. Some of the existing table driven or proactive protocols are: DSDV and ZRP.

3.2. On Demand or Reactive Protocols

In these protocols, routes are created as and when required. When a transmission occurs from source to destination, it invokes the route discovery procedure. The route remains valid till destination is achieved or until the route is no longer needed. Some of the existing on demand routing protocols are: DSR and AODV.

4. Destination Sequence Distance Vector (DSDV)

DSDV [3]-[4] is based on the bellman ford algorithm and developed by Charles E. Perkins and Pravin Bhagwat in 1994. Packets are transmission between mobile nodes by using routing tables which are stored at Mobile node. Each routing table, at each of the mobile node contain list of all available destinations, and the number of hops to each. Each route table entry is tagged with a sequence number which is originated by the destination station. To achieve the consistency in the dynamically changing topology based network, every mobile node periodically transmits updates and routing tables are updated. Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically and incrementally as topological changes are detected. Consider Node A wants to send a data to Node C as shown in Figure 1, but Node C is not in the coverage area of Node A. Hence it has to forward packet to Node B and Routing table of Node B comes into picture, it will act as routing agency for forwarding packet from Node A to Node C.

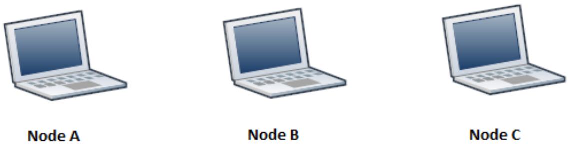

Fig 1: Mobile Ad Hoc Network

Routing table contain destination IP address, next hop, number of hops, sequence number and install time. Routing Table of Node B will be as shown in table 1.

Consider MH_4 in Figure 2. Table 2 shows a possible structure of the forwarding table which is maintained at MH_4.Suppose the address of each Mobile Host is represented as MH_i Suppose further that all sequence numbers are denoted SNNN_MH_i, where MH_i specifies the computer that created the sequence number and SNNN is a sequence number value.

Destination	Next Hop	No. of Hops	Seq. No.	Install Time
A	A	0	A 46	001000
B	B	1	B 36	001200
C	B	2	C 28	001500

Table 1: Routing Table for Node B

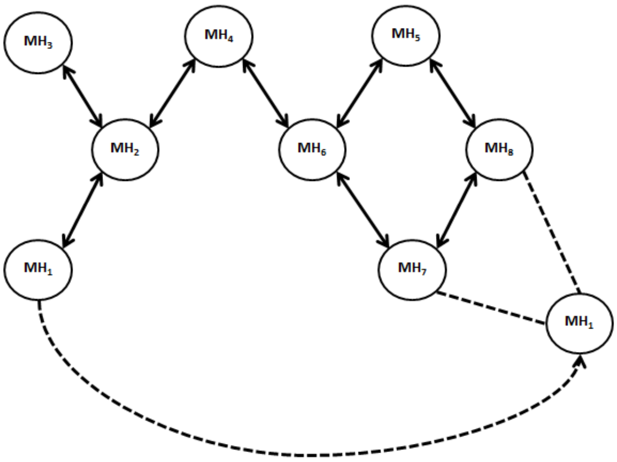

Fig 2: Movement in an ad-hoc network

Destination	Next Hop	Metric	Sequence number	Install
MH_1	MH_2	2	S406_ MH_1	T01_ MH_4
MH_2	MH_2	1	S128_ MH_2	T01_ MH_4
MH_3	MH_2	2	S564_ MH_3	T01_ MH_4
MH_4	MH_4	0	S710_ MH_4	T01_ MH_4
MH_5	MH_6	2	S392_ MH_5	T02_ MH_4
MH_6	MH_6	1	S076_ MH_6	T01_ MH_4
MH_7	MH_6	2	S128_ MH_7	T02_ MH_4
MH_8	MH_6	3	S050_ MH_8	T02_ MH_4

Table 2: Structure of the MH_4 forwarding table

Suppose that there are entries for all other Mobile Hosts, with sequence numbers SNNN_MH$_i$, before MH$_1$ moves away from MH$_2$. The install time field helps determine when to delete stale routes. With our protocol, the deletion of stale routes should rarely occur, since the detection of link breakages should propagate through the ad-hoc network immediately. Nevertheless, we expect to continue to monitor for the existence of stale routes and take appropriate action.

Destination	Metric	Sequence number
MH$_1$	2	S406_ MH$_1$
MH$_2$	1	S128_ MH$_2$
MH$_3$	2	S564_ MH$_3$
MH$_4$	0	S710_ MH$_4$
MH$_5$	2	S392_ MH$_5$
MH$_6$	1	S076_ MH$_6$
MH$_7$	2	S128_ MH$_7$
MH$_8$	3	S050_ MH$_8$

Table 3: Advertised route table by MH$_4$

From table 2, one could surmise, for instance, that all the computers became available to MH$_4$ at about the same time, since its install-time for most of them is about the same. One could also surmise that none of the links between the computers were broken, because all of the sequence number fields have times with even digits in the units place. Table 3 shows the structure of the advertised route table by MH$_4$.

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

The AODV [5] routing protocol is a reactive routing protocol. Therefore, routes are determined only when needed. Whenever an AODV router or node receives a request to send a message, it checks its routing table for route existence. Each routing table entry consists of Destination address, Next hop address, Destination sequence number, Hop count. If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a message queue, and then it initiates a route request to determine a route. Upon receipt of the routing information, it updates its routing table and sends the queued message(s). AODV nodes use four types of messages to communicate among each other. Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance. The following sections describe route determination and route maintenance in greater detail. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen.

5.1. Route Request (RREQ)

<table>
<tr><td>Type</td><td>J</td><td>R</td><td>G</td><td>D</td><td>U</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="8">RREQ ID</td></tr>
<tr><td colspan="8">Destination IP Address</td></tr>
<tr><td colspan="8">Destination Sequence Number</td></tr>
<tr><td colspan="8">Originator IP Address</td></tr>
<tr><td colspan="8">Originator Sequence Number</td></tr>
</table>

Fig 3: Root Request

The format of the Route Request message is illustrated in Fig 3, and contains the following fields: Type is 1,J is Join flag reserved for multicast, R is Repair flag reserved for multicast, G is Gratuitous RREP flag indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field, D is Destination only flag indicates only the destination may respond to this RREQ, U is Unknown sequence number indicates the destination sequence number is unknown, Reserved Sent as 0 i.e. ignored on reception, Hop Count The number of hops from the Originator IP Address to the node handling the request, RREQ ID is sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address, Destination IP Address is the IP address of the destination for which a route is desired, Destination Sequence Number is the latest sequence number received in the past by the originator for any route towards the Destination, Originator IP Address is the IP address of the node which originated the Route Request, Originator Sequence Number is the current sequence number to be used in the route entry pointing towards the originator of the route request.

5.2. Route Reply (RREP)

<table>
<tr><td>Type</td><td>R</td><td>A</td><td>Reserved</td><td>Prefix Sz</td><td>Hop Count</td></tr>
<tr><td colspan="6">RREQ ID</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="6">Destination Sequence Number</td></tr>
<tr><td colspan="6">Originator IP Address</td></tr>
<tr><td colspan="6">Originator Sequence Number</td></tr>
</table>

Fig 4: Root reply

The format of the Route Reply message is illustrated in Figure 4, and contains the following fields: Type is 2 for RREP, A Acknowledgment required, Prefix Size If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix as the requested destination, Lifetime is the time in milliseconds for which nodes receiving the RREP consider the route to be valid and all other fields are same as in RREQ packet format.

5.3. Route Error (RERR)

Type	N	Reserved	Destination Count
RREQ ID			
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Option			

Fig 5: Root Error

The format of the Route Error message is illustrated in Figure 5, and contains the following fields: Type is 3, N is No delete flag set when a node has performed a local repair of a link, and upstream nodes should not delete the route, Reserved Sent as 0, DestCount is the number of unreachable destinations included in the message MUST be at least 1, Unreachable Destination IP Address is the IP address of the destination that has become unreachable due to a link break, Unreachable Destination Sequence Number is the sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

5.4. Route Reply Acknowledgment (RREP-ACK)

Type	Reserved

Fig 6: Route Reply Acknowledgment

The format of the Route Reply Acknowledgment illustrated in Figure 6, and contains the following fields: Type is 4 and Reserved Sent as 0.

6. Dynamic Source Routing (DSR)

The DSR [6] Protocol is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes cooperate to forward packets for each other to allow communication over multiple “hops” between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR Routing Protocol. Because the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing. The DSR Protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use. While designing DSR, we needed to create a routing protocol that had very low overhead yet was able to react quickly to changes in the network, providing highly reactive service to help ensure successful delivery of data packets in spite of node movement or other changes in network conditions.

7. Performance Metrics

If we want to compare some of the protocols then, we have to consider some of the metric for comparing the performance of the protocols. Performance metrics [7]-[9] as:

7.1. Packet Delivery Fraction

It is the ratio of the data packets delivered to the destinations to those generated by the sources.

7.2. Throughput

Throughput of the routing protocol means that in certain time the total size of useful packets that received at all the destination nodes.

7.3. Average End-To-End Delay

Average End-to-End delay (seconds) is the average time it takes a data packet to reach the destination.

7.4. Routing Overhead

Average routing overhead is the total number of routing packets divided by total number of delivered data packets.

7.5. Jitter

The delay variation between each received data packets.

7.6. Packet loss ratio

The ratio of the data packets originated by the sources fails to deliver to the destination.

8. Conclusion

This paper totally speaks about working of reactive and proactive protocols and every protocol has its advantages and disadvantages in particular scenario of network. Some time they may work better and some time not. Many of the research paper have been focused on performance metric for comparing the performance of routing protocols. Performance metric like packet delivery ratio, throughput, average end to end delay and routing overhead. For simulation of routing protocols in MANET mostly used simulation tools are ns-2, netsim and qualnet. But, most of the researchers preferred tool is ns-2. There are many issues that require further investigation like traffic control, power control and security. In case of security, due to the broadcast nature of the wireless node security becomes more difficult. Further research is needed to investigate how to stop an intruder from joining an ongoing session or stop a node from receiving packets from other sessions.

9. References

[1] J. Macker and S. Corson, “Mobile Ad Hoc Networks (MANET),” IETF WG Charter., http://www.ietf.org/html.charters/manet-charter.html, 1997.
[2] E. M. Royer and Chai-Keong Toh, “A Review of current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, April, 1999.
[3] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers”, Computer Communication Review, vol. 24, 1994.
[4] Singh Rajeshwar, Singh Dharmendra K. and Kumar Lalan, “Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks” International Journal Advanced Networking and Applications, Volume: 02, Issue: 04, 2011, page: 732-737.
[5] C.E. Perkins and E.M. Royer, “Ad-Hoc on-Demand Distance Vector Routing,” Proc. Workshop Mobile Computing Systems and Applications (WMCSA ’99), Feb. 1999.
[6] J. Broch, D. B. Johnson and D. A. Maltz, “The dynamic source routing protocol for mobile ad hoc networks,” draft-ietf-manetdsr-01.txt, Dec. 1998.
[7] A. A. A. Radwan, T. M. Mahmoud and E. H. Houssein, “Evalution comparision of some ad hoc networks routing protocols,” Egyptian Informatics Journal, Jan. 2011, page: 95-106.
[8] Li Layuan, Li Chunlin and Yaun Peiyan, “Performance Evaluation and Simulation of Routing Protocols,” Computer Communications, Feb. 2007, page: 1890-1898.
[9] Charles E. Perkins, Elizabeth M. Royer,Samir R. Das and Mahesh K. Marina, “Performance Comparision of Two On-Demand Routing Protocols for Ad Hoc Networks,” IEEE Personal Communications, Feb. 2001.
[10] Duyen Trung H, Benjapolakul W and Minh Duc P, “Performance evaluation and comparison of different ad hoc routing protocols,” Elsevier Computing Communication, 2007, page: 2478–2496.