ISSN:0975-9646

Diminution of Packet Drop by Efficient Selection of Network Route in MANET

Manish V M , J Vaijayanthimala

Department of Computer Science,
Mahendra Engineering College, Salem
India

Abstract. Om the beginning of the twentieth century Mobile ad hoc network (MANET) is the popular and promising area of research. Due to the immense growth of wireless devices wireless network especially MANET has become interesting area of researchers. MANET [1] is a self configured and self centered network with highly dynamic topology. Each node in the network can act as either router or source. Due to the dynamicity of topology the route failure is very common and crucial issue in MANET. Routing is the major issue in MANET since there is no central coordinator to control the routing. Control is distributed among nodes. MANET is a stand alone network and any node can join and leave the network anytime. With this property the "any time anywhere networking" came into reality. Because of the wireless error prone medium packet loss is very large in MANET. This is not only because of the congestion but also due to high error rate, collision and high probability of link breakage. As per the study packet loss became an important aspect of diminishing the performance of the network and also it is not predictable. The main objective of this paper is to study the reason for packet loss and tries to reduce the same. This paper evokes a new approach to reduce the packet drop by efficient selection of route for communication.

Keywords: MANET, AODV, Route stability,

1 INTRODUCTION

The rapid deployment of mobile devices and the increased usage of those devices need the independent self organized network without any central coordination. The network should be survivable, efficient, dynamic communication capability for emergency/ disaster situations and reusable. This raised the significance of mobile ad hoc network (MANET).

MANET is a self organized network with collection of autonomous mobile nodes. The nodes can be communicated through wireless media. Since the nodes are highly mobile the network topology is may change rapidly and unpredictable over time. The nodes in the network are responsible for discovering the route and delivering the message. The applications of MANET[1] are diverse and are ranging from small to large high mobile network so the design of the routing protocol is a major issue. Because of the decentralized nature the routing protocol for static network can not be directly applied for MANET. Properties of wireless media such as propagation path loss, fading, multi user interference, bandwidth constraint, error prone medium and the like are directly affected the performance of the network. The network should be able to adaptively alter the routing paths to alleviate any of those issues.

Routing protocols for MANET are broadly classified into proactive, reactive and hybrid. Proactive or table driven protocol is the extension of the protocol which we are using in static network. The routing table is created when the network is configured and this table is exchanged periodically. Each node update it's routing table according the information gain from it's neighbors. Wireless routing protocol (WRP), Destination sequenced distance vector (DSDV)[2] are some example protocols of this type. Periodic exchange of routing table induces network overhead significantly. This can be reduced by using reactive or on demand protocols. In the reactive protocol the routes are computed only when a node wants to send a message to any destination. The routing tables are not periodically interchanged. Ad hoc on demand distance vector (AODV) [2], Dynamic source routing (DSR)[2] are reactive routing protocols.

In the table driven protocol the routing information is readily available and there will not be any delay for discovering the routes. But in the reactive protocol the routes has to be find out when it is needed. This is done through some control messages like RREQ and RREP etc. This takes some delay. Take the advantages of reactive and proactive protocols the third category hybrid protocols are introduced. Zone routing protocol (ZRP) is a classical example of hybrid routing protocol.

This paper examines the impact of packet loss during the communication by using AODV protocol. Because of the error prone medium the packet loss is very high in MANET. Some nodes intentionally drop the packet and during the route computing process the possibility of packet drop can also be taken into account. The reason for packet drop is studied and proposes a method for reducing the packet drop by efficiently select the route from source to destination..

The rest of this paper is organized as follows. Section 2 elaborates Route selection process in AODV. Section 3 describes the impact of packet drop and related works. Selection of shortest path with the consideration of packet drop is discussed in section 4 and a conclusion is given in section 5.

2 BRIEFING OF ROUTE SELECTION IN AODV

Route selection is an important and necessary process in the routing scenario in ad hoc network. The topology is the MANET is frequently changed so that the routing algorithm must be efficient to cope up with the dynamic changes in the topology. In the proactive approach the

routing overhead is very high and route table information can be stale. This problems are avoided in the on demand routing protocols. Still there are problems exists like number of control packets, reroute establishment delay etc. In AODV protocol the route establishment and route maintenance is the two important functions. The route establishment is based on the demand of the node and the route is maintained in the algorithm whenever there is a route break occurs. Because of the route instability re route establishment is frequently needed in MANET. Even though the route table information flooding is eliminated in the on demand routing protocol but the control information is flooded in the network is very high. The route failure creates overhead due to reroute establishment delay. This paper studies the importance of route selection in AODV and tries to improve the selection of route to reach destination based on the past behavior of the network.

During the route establishment phase in AODV[1] the node wants to send message is generated a route request (RREQ) control packet and send to it's neighbor nodes. Each node send this message to their own neighbors and this process is continued till reaches the destination. The destination node creates a route relay (RREP) message and sends back to the source node. RREP contains the information about the route to the destination so the source can send data to the destination. Normal algorithm for the route selection in AODV is shortest path algorithm and it is depend on the number hops in the route. This is not suitable in all the cases because some of the nodes in the route may have small queue size and they may dropping many number of packets or they may intentionally drop the packets during the communication.

Due to the limitation of wireless link the link breaks are very frequent and the existence of the neighbors is detected by using beaconing message. The HELLO beacons are periodically sent by each node and check for the responses. If there is no response then assumes that the link between that two nodes are broken and the detected node creates an error message (RERR) and also flooded in the network. If the source node detects the RERR message it again starts the route discovery. This leads wastage of resources. The main resource contain in MANET is battery life. For re route establishment and route computation lots of energy is wasted. The route selection process in AODV is depicted in the figure1.

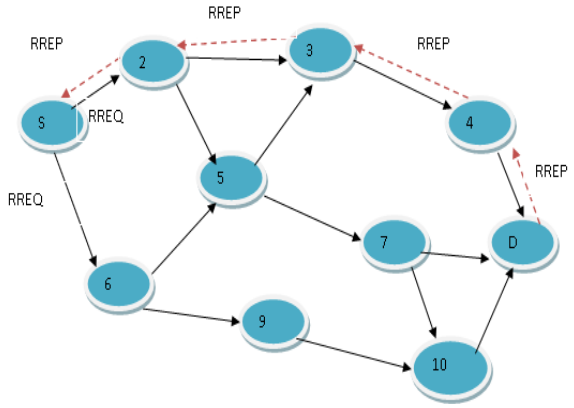

Figure 1: Route selection in AODV

In AODV route selection based on the number of hops. Consider the figure 1 there are various routes to reach destination form node S. S node creates RREQ message and circulates. This message containing the destination id which used to determine the freshness of the route. The request reaches the destination node D then it creates the RREP message sending to the source S and following the same route. The destination creates only one RREP message in respect of one RREQ. It is always depends on the time with which the RREQ message reached at the destination.

3 Impact Of Packet Drop In Route Selection

On demand routing algorithm like AODV minimize the network overhead than proactive routing protocol. Packet drop [8] [9] is a major constraint that diminishes the performance of the network. Packet drop can occur in many ways. Congestion at the route, buffer overflow, link instability are some normal reasons. Some nodes act as malicious nodes and those nodes intentionally drop the packet. Packet drop significantly reduce the performance of the whole network. Even if the route selected is the optimized one, due to the packet drop the network does not perform up to the level.

Packet drop can be happened in two ways. Nodes are purposely discarding the packets with no reasons and the packets can be dropped because of insufficient resources. Most of the time the packet drop occurs because of the congestion in the network. There will not be any buffers space to accommodate the incoming packets then those packets are discarded. But in other case some of the nodes are malicious and they are not willing to forward the packets to next nodes. These nodes are simply discarding the packets. The existence of the malicious nodes significantly degrades the performance of the network. If the number of packet drop increases then the packet delivery ratio (PDR) decreases. Several algorithms designed for determining the malicious node in the network. Many algorithms concentrate on finding the malicious node and then this can be avoided for packet forwarding. Detection of malicious nodes based on packet drop. If the number of packets dropped by any node is grater than a given threshold it is identified as malicious and the report of the malicious node is generated and flood this information in the network.

Avoiding the malicious node in between the routing is not a solution for improving the performance. If this can be identified when the new route is calculated then we can improve the performance of the network.

4 Selection Of Shortest Route With The Consideration Of Packet Drop In Each Node In The Path

In any on demand routing protocol the route is explored at the time of data send. This protocols always tries to select the shortest path and send the data through this path. In all existing algorithm route selection does not consider the malicious nodes in the network. Packet drop is a crucial factor for the performance of the network. If the packet drop is very high then packet delivery ratio is decreases

thereby decreasing the throughput. In this proposed scheme the packet drop of each node is considered as criteria for finding the shortest path from source to destination. If the packet drop is above the threshold value that node does not considered as a forwarder node. This can be find out by feedback mechanism. After getting each packet every node send ACK message to the sender. In AODV algorithm normally the destination node sends the ACK. But in the new scheme every node sends the ACK back to the sender after its successful reception of a packet. ACK coming from the destination and ACk from the neighbor node is compared to get the right information about the packet drop. If the response from both side is same then the neighboring node is dropped the packets due to some other reasons. So it is not blacklisted as malicious. Otherwise the node is purposely dropped the packet and is identified as malicious node. Fig 3 gives a model for the scheme. Node N1 checks the ACK from node N2 and N5. Similarly each node compares the ACK message it received.

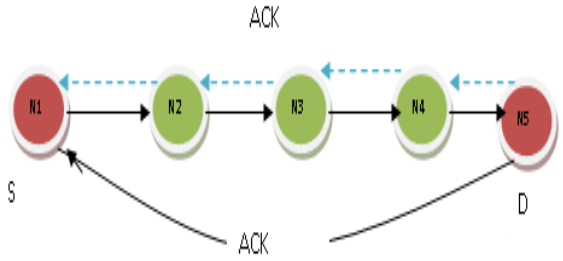

Fig 3: Model for Malicious Node Identification

The following subsections describe the algorithm for determination of malicious node, data structures used for implementing the algorithm.

A. ALGORITHM

/* Determination of malicious node */

For each node calculate the following
Number of packet dropped > threshold
Add the nodes into Black list

```
If (each node in the black list)
{
        Node X checks ACK // X is the black listed node
        if ( any ACK is missing from neighbor nodes)
        {
                Check the ACK from destination
                Comp( ACKneighbor, ACKdestination)
                    {
                        If(( ACK neighbor – ACKdestination)=5)
                            Add node into malicious node list (MNL)
                            Else
                            Break;
                }
        }
}
```

B. Data Structures

Various data structures are needed for implementing the algorithm. Each node is associated with a black list table and malicious node table. Each node identify the malicious node after a particular number of trails. Weighted averaging technique is used for calculating this. First check whether the neighbor nodes are black listed or not. From the black listed nodes malicious nodes are identified by comparing the ACk message from neighbors and destination and it is entered into the malicious node list.

Black listed Node
N2
N3

Table 1: black listed node detected by node N1

Malicious Node
N2
N3

Table 2: Malicious node detected by node N2

5 CONCLUSION

Packet drop is a major factor to degrade the performance of the network. Some malicious nodes purposely drop the packets and some other nodes drop the packets because of the insufficient resources. This paper tries to find out a method to differentiate those nodes and consider the packet drop in the route determination mechanism. Even though some overhead is induced in the network due to the ACK message but this is efficient in terms of route failure. We are considering the packet drop during the route creation and the route might be stable This paper gives a clear idea of route failure in the network and the disadvantages of the mechanism adopted to withstand this in the normal AODV. The new approach has been designed to minimize packet drop in the network. This also ensures the performance enhancement in terms of throughput by reducing the number of dropped packets. The approach outlined above does not have any additional computational complexity and this uses the same principle of AODV protocol which is universally accepted.

REFERENCES

1. Jayesh Kataria, P.S. Dhekne, Sugata Sanyal,"Ad Hoc On-Demand Distance Vector Routing with Controlled Route Requests", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 1, No. 1, pp 9-15, June 2007, Serial Publications
2. George Aggelou, "Mobile Adhoc Networks", Tata McGraw-Hill, 2009 ISBN-13:978-0-07-067748-7.
3. G.S. Tomar; Member IEEE, "Modified Routing Algorithm for AODV in Constrained Conditions", Second Asia International Conference on Modelling & Simulation, IEEE, 2008
4. Perkins CE, Royer EM "Ad-hoc on-demand distance vector routing". In the Proceedings of IEEE WMCSA, pp. 90 –100, 19993.
5. Charles E. Perkins, Elizabeth M. Royer, "Ad-Hoc on Demand Distance Vector Routing." Prac. 2nd IEEE FVksp. Mobile Computing and Applications, pp. 90-100, Feb. 1999.
6. Hong Jiang, Garcia-Luna-Aceves, J.J. "Performance comparison of three routing protocols for ad hoc networks". Proceedings of the tenth International Conference on Computer communications and Networks, Oct 2001, pp. 547-554

7. Malicious Node Detection System for Mobile Ad hoc Networks, A Rajaram, Dr S palanisami,(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85
8. Detecting Selfish and Malicious Nodes in MANETs, Martin Schütte, Seminar: Sicherheit In Selbstorganisierenden Netzen, Hpi/Universität Potsdam, Sommer semester 2006
9. Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, Aishwarya Sagar Anand Ukey, Meenu Chawla, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010