Reliable Routing in Aodv Protocol

Nilesh M.Kadivar
Dept. of Computer science & Engineering
B.H. Gardi College of Engineering & Technology, Rajkot, Gujarat, India

Abstract--- Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Ad hoc Networks more vulnerable due to various security attacks which affects many performance parameter like PDR, Throughput and Delay. To accomplish our goal, we have develop virtual currency based approach to improve perfomance by detecting attack and remove its effect and multiple blackhole node affect more in perfomance

Keywords*:* MANET, blackhole,AODV,DSDV , DoS, routing, Scheme

I. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi hop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [2].

Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities[11]. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks.

II. AODV ROUTING IN MANET

From the comparisons discussed in last section, it is clear that overall AODV is a standard reactive protocol which is better than other reactive routing protocols like DSR, or Proactive Routing Protocols like DSDV. The Ad-hoc on demand distance vector (AODV) routing algorithm is a routing protocol designed for Ad-hoc mobile devices. AODV is Combination of DSR and DSDV.

- It has on-demand mechanism of route discovery and route-maintenance from DSR.
- Plus the hop-by-hop routing, sequence numbers and periodic beacons from DSDV.

Basically working of AODV can be divided into two phase: Route Discovery Phase for discovering the route to the node to which data is to be sent and Route Maintenance Phase is for maintaining the route once it is established between source and destination.

A. Route discovery process

When a node has data to send to another node but it does not have any routing information i.e. Route to the destination, Route Discovery process is started. Source node who wants to send the data will generate RREQ packet and broadcast it to its neighbours. Each intermediate node which does not have route to the destination, will also broadcast RREQ packet. To avoid the unnecessary flooding of RREQ, first RREQ will be considered and each subsequent duplicate RREQ packet will be discarded.

Each intermediate node will cache the route back to the originator if it does not have any route to the originator or the received RREQ gives fresh and shorter path than that of already cached path. This rout caching mechanism is called Reverse path setup. Reverse path is setup to unicast RREP back to the source from the destination or the intermediate node that have the fresh route to the destination.

If the node does not have fresh enough route to the destination of RREQ, it will rebroadcast it. Otherwise it will

send RREP to the source. After receiving first RREQ packet, destination node generates RREP packet and unicast it to the originator.

Every intermediate node receiving RREP, will establish a route to the destination which is called Forward path setup. When source receives RREP packet, route is established in hop by hop fashion. And now source sends data to the destination which will be delivered to the destination hop by hop fashion.

B. Route maintenance

When a link break in an active route occurs, the upstream node of that break may choose to repair the link locally based on its distance to the source or destination. If it is near to the destination than source, it will do local route repair of the link. Otherwise it will send RERR message to the Source initiating route discovery.

To repair the link break, upstream node of the link breakage initiates route discovery for the destination. During local repair data packets should be buffered. If, at the end of the discovery period, the repairing node has not received a RREP (or other control message creating or updating the route) for that destination, it transmits a RERR message for that destination to the source. .

RERR message can be broadcasted or it can be unicast to the source. Each node receiving RERR message will check for unreachable destination in route table and will make it down if the transmitter of the RERR message is used as next hop for that destination. If such an

entry found in the route table, then only it will broadcast of forward the message

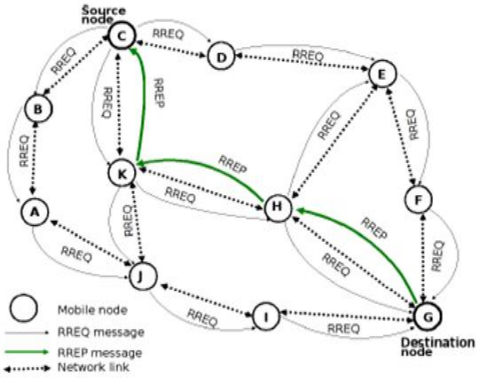

Fig. 1**:**

III. Black Hole Attack

The backhole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets.

In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighbouring nodes that monitor the ongoing packets.

In *Below Figure* Node 1 Wants To Send Data Packets To Node 4 And Initiates The Route Discovery Process. We Assume That Node 3 Is A Malicious Node And It Claims That It Has Route To The Destination Whenever It Receives Rreq Packets, And Immediately Sends The Response To Node 1. If The Response From The Node 3 Reaches First To Node 1 Then Node 1 Thinks That The Route Discovery Is Complete, Ignores All Other Reply Messages And Begins To Send Data Packets To Node 3. As A Result, All Packets Through The Malicious Node Is Consumed Or Lost [10]

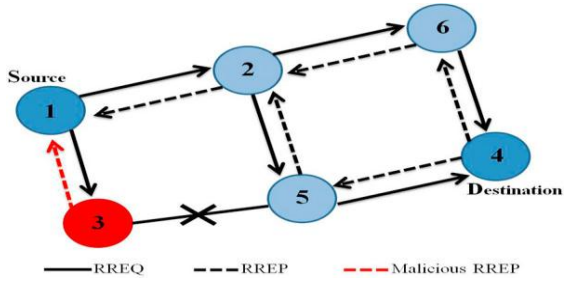

Fig. 2:

IV. Proposed Approach Based On Virtual Currency

A. Algorithm to apply virtual currency based approach

1. Initialize all the node with some amount of Virtual currency and set the packet drop index as zero.
2. During Packet Forwarding Mechanism if node is forwarding the packet successfully than increase the Virtual currency by two unit else Drop() function will be called and reduce the virtual money by two unit and increase the drop index.
3. Now set the Minimum Threshold value of virtual currency and than check following condition.

if (virtual currency <min Threshold)
{
Discard the node from Route for this give them runtime mobility using Setdest()
function
} OR
if(Drop[index] > Threshold)
{ Discard the node from Route for this give them runtime mobility using Setdest()
Function
}

V. Simulation And Result

Parameter	value
Simulation area	1000*1000
Simulator	NS-2.35
Number of node	25
Communication traffic	CBR
Simulation time	200s
Max. connection used	5,10,15,20
Pause time	10s
Protocol used	AODV
Max speed of node	5,10,15,20 m/s

we have compare the throughput.,pdr and end to end delay as perfomance parameter of standard aodv protocol with blackhole attacked aodv and virtual currency based aodv which we have proposed method.analyzed simulated result shown in graph..b-throughput indicate blackhole throughput, vc-throughput indicate virtual currency throughput

Experiment 1: Throughput

Throughput: It is the average rate of successful message delivery over a communication channel in bits/sec

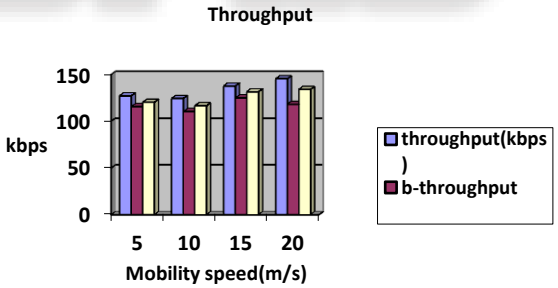

Fig. 3:

Experiment 2: PDR

Packet Delivery Ratio (PDR): It is defined as the ratio of total number of packets that have reached the destination node to the total number of packets created at the source node

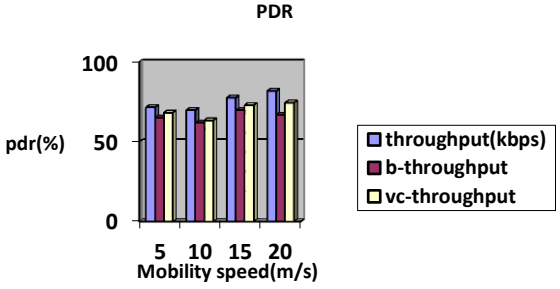

Fig. 4:

Experiment 3:End to End Delay

End-to-end Delay: It is defined as time taken for a packet to be transmitted across network from source to destination. The metric should have lower value for the efficient network.

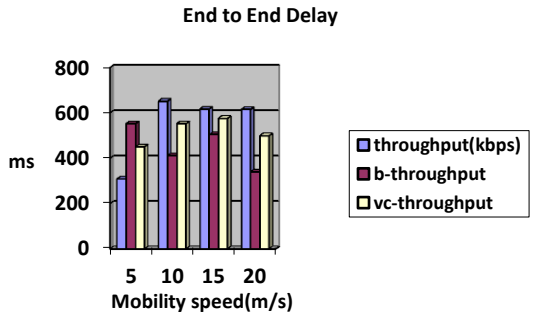

Fig. 5:

Experiment 4: No of Blackhole Node

In this experiment we have checked blackhole node effect when blackhole node increases perfomance are decreases

In experiment 1,2,3 we have used one blackhole node effect in topology

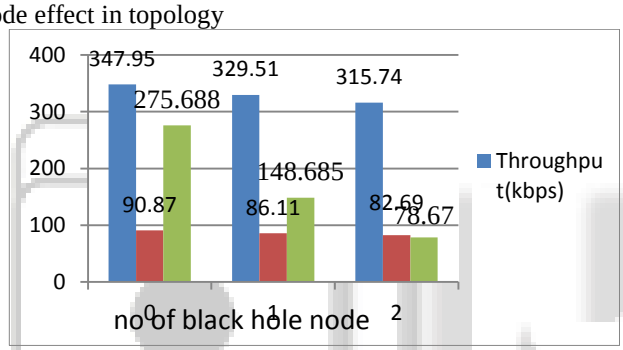

Fig. 6:

VI. Conclusion

Using proposed approach we can detect the block hole attack and by preventing it using virtual currency based approach different parameter like PDR, Throughput, delay can be measured and improvement in this parameter can see by comparing the result. we have get the better result when aodv protocol is under attack by blackhole due to our approach

References

[1] Lyes Khoukhi, Hakim Badis, Leila Merghem-Boulahia1 and Moez Esseghir "Admission control in wireless ad hoc networks " EURASIP Journal on Wireless Communications and Networking, 2013,pp- 1-109

[2] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. "Scalable routing protocols for mobile ad hoc networks", Journal of Network, IEEE, Jul/Aug 2002, pp. 11-21

[3] Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) "Optimized Link State Routing Protocol for Ad Hoc Networks." International Conferenceon Technology for the 21st Century,Pakistan,2001

[4] G.Vijaya Kumar, Y.Vasudeva Reddyr , Dr.M.Nagendra, "Current Research Work on Routing Protocols for MANET: A Literature Survey", International Journal on Computer Science and Engineering, 2010, pp. 706-713

[5] Guangyu Pei, Gerla, M., Tsu-Wei Chen, "Fisheye state routing: a routing scheme for ad hoc wireless networks", International Conference on Communications, New Orleans, LA, Jun 2000

[6] PerkinsCE, Bhagwat P "Highly Dynamic Destination-Sequenced Distance-Vector Routing(DSDV)for Mobile Computers.", Conference on Communications Architectures, Protocols and Applications, London, UK,1994,pp. 234-244

[7] Elizabeth M., Samir R., Charles E. Perkins "Ad hoc On-Demand Distance Vector (AODV) Routing draft-ietf-manet-aodv-13.txt" INTERNET DRAFT Nokia Research Center 17 February 2003

[8] David B. Johnson and David A. Maltz. "Dynamic source routing in ad hocwireless networks.", Technical report, Carnegie Mellon University, 1996.

[9] Jao-Ng M, Lu I-T "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks." IEEE Journal on Selected Areas in Communications, Aug 1999, pp. 1415- 1425

[10] Chanchal Aghi1, Chander Diwaker " Black hole attack in AODV routing protocol: A Review"April-2013,pp-820-823

[11] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", 6th annual international conference on Mobile computing and networking, pp.243-254, 2000

