ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET

Aman Saurabh[1],Rakesh Yadav[2], Harjeet Kaur[3]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Punjab, India[1]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Punjab, India[2]

Assistant Professor, Department of Computer Engineering, Lovely Professional University, Punjab, India[3]

ABSTRACT: A mobile ad hoc network can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. The security in MANET is a highly preferred research area these days because it is susceptible to various attacks like multiple black hole attack which we are discussing in this paper. A Multiple Black Hole Attack is a type of DOS attack which effects network load, packet end to end delay and network throughput. This paper investigates the study of AODV protocol under Multiple Black Hole Attack. This approach can be used to detect multiple black hole nodes present in an ad hoc network. The purpose of the designed algorithm is to avail stability in the network when it is under attack by multiple malicious nodes, maintaining a reasonable level of packet end to end delay, packet loss & throughput. It will also help in maintaining a secure passage to destination. In this algorithm we make use of the knowledge based learning & Bogus RREQ to validate each node in its path thereby providing a direct negotiation for secure route.

KEYWORDS: MANET, Security, Malicious node, Black Hole Node, AODV.

I. INTRODUCTION

A MANET can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. In this type of network the devices communicate through a wireless medium with each other. It is necessary that the devices present in the network should cooperate with each other so the packets can be transmitted via the intermediate devices when there is no direct path from the source to the destination. There is no concept of central controlling authority & a permanent network infrastructure in a mobile ad-hoc network. Transfer of packets is done with the help of routing protocols, which help in determining the suitable route from source to destination for initiating as well as maintaining a connection between the two. Network topologies are dynamic in nature, due to which there are link breakage and disruption in peer to peer connection. There is highly dynamic in nature of wireless network imposes severe restrictions on routing protocols. Ad hoc network can be described as a wireless network which works without the existence of a centralized and fixed infrastructure. Without the presence of an infrastructure, there exist various issues & challenges in the working of these wireless ad hoc networks. Thus a wireless network consisting of mobile nodes which is ad hoc in nature can be called as MANET. The mobile nodes in the network are capable to acknowledge & course traffic via the intermediate nodes towards the destination, mobile nodes present in the network can act as a router as well as a host. The frequent fading of mobile nodes results in connection termination and re-association of nodes includes another variable to the characteristics of mobile nodes which is energy.

As MANETs are illustrated by limited bandwidth and node mobility, it is suggested to consider how much energy efficient a mobile node is and frequent changes in the topology and reliability of the communication in the scheme. There are many types of protocols are available in MANET. A routing protocol's efficiency can be evaluated on the basis of battery power utilized by a mobile node participating in the communication in order to route the traffic in the network.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

1.1 Routing Protocol:

The principle objective of routing protocols in ad-hoc network is to create optimal path i.e. having lesser intermediary nodes between source and destination with least overhead and least transfer speed utilization so that the data packets are passed on time. Protocols used in MANET should be able to perform in an effective & efficient manner over a variety of heterogeneous networking environment including small ad-hoc group as well as multi hop networks which are larger in size. In reference to the routing topology of MANET, routing protocols in MANETs can be classified into proactive, reactive and hybrid. Proactive protocols constantly maintain the updated topology of the network and are typically table-driven. The Proactive routing protocols include DSDV. Reactive protocols are also known as source-initiated on-demand protocols, they do not periodically update the routing information. They initiate route discovery process only when they are requested to do so, source node wants to find a path to a desired destination. AODV & DSR are some example of these types of protocols. Now coming to hybrid protocols, they utilize the functionality of both the protocols i.e., reactive and proactive approaches. Zone Routing Protocol is an example of hybrid routing protocol.

1.2 Attacks in MANET:

1.2.1 Wormhole Attack

The worm hole attack is quite typical and merciless attacks, which can be executed in MANET. In this type of attack message is captured from the one region of network and replaying in other region. Attacker creates tunnel between two nodes which participate for communication. One attacker gather all message and other attacker replay to misinterpret to make destination unreachable from network.

1.2.2 Black hole Attack

In black-hole attack malicious node use its routing protocol to know other node that it has shortest path towards destination and attacker drop the packet to reduce the quantity of information is available to other node. This type of attack made intentionally for denial of service type attack. This make destination system unreachable or shutdown in network.

1.2.3Byzantine Attack

In this type of attack, there are multiple malicious node which works in collision to create routing loops, transmitting the packet through sub optimal routes as well as dropping of packets.

1.2.4Gray hole Attack

It is also known as selective packet drop attack because it drops the packet selectively with certain probability. The gray hole node works in such a way that for an instance it will act as malicious & then it will switch back to being a normal node.

1.2.5 Denial of Service Attack

The main motive behind this attack is to make the network resource unavailable to the nodes present in the network. On the successful execution of the attack, the network resources will be inaccessible. The techniques used by attacker to perform a successful DOS attack in MANET includes jamming of radio signals& making the mobile nodes run out of battery.

II. BACKGROUND AND RELATED WORK

Sanjay Ramaswamy, et al were the first who proposed a solution for identifying multiple black hole nodes working in cooperation [6]. They somewhat modified AODV protocol by presenting cross checking and data routing information table (DRI). In which the table maintained every single entry of the node. For the transfer of the packets the authors relied on the trusted nodes.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

The black hole issue is a security attack that occurs in mobile ad hoc networks (MANETs). There are two possible solutions presented by Mohammad Al-Shurman et al. The first solution is to determine multiple routes to reach the destination [2]. Whereas the second solution is the exploitation of the sequence number present in the header of routing packets. On simulating the solutions it is observed that compared to the typical AODV routing scheme; the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

Some enhancement in the existing AODV protocol is introduced by Latha Tamilselvan et al [1] which are able to avoid multiple black holes. In order to identify multiple black holes cooperating with each other technique is given to discover the safe route by avoiding the attacks. An assumption was made by the researchers while giving the solution for the concerned issue is that nodes are authenticated in advance and therefore they are allowed to participate in the communication passage. It uses Fidelity table where every node that is participating is given a loyalty level that will provide trustworthiness of that node. In the fidelity table, nodes which are having 0 values is are considered as adversary nodes and is thus eliminated.

An IDAD is introduced by Yibeltal Fantahun Alem et al to prevent both single as well as multiple black hole nodes [7]. It works on the principle that the mobile nodes present in the network do not trust on the other nodes to avoid intrusion. IDAD consists of audit data which is the pre-collected set of anomaly actions. If the action (activity) of a node is identical to the actions then the system forbids the particular node. On simulating the proposed system, it is observed that it maximizes the network performance by decreasing the control packet generation.

The advanced routing methods are discussed by Fan-Hsun et al. They not only categorize these proposals into single black hole attack and collaborative black hole attack but also analyzed the classes of these solutions and provided the comparison table. They presented the summary of pros and cons with popular routing protocol in wireless mobile ad hoc networks [9]. Then, the routing methods of existing solutions are categorized and discussed. In this work, it is observed that there are specialized skills in both proactive routing and reactive routing. The proactive detection method has the superior detection probability &the packet delivery ratio, but the major drawback in it is the higher routing overhead because the broadcast packets is done periodically. The routing overhead problem was removed by reactive detection method, but in the beginning of routing procedure it suffered from some packet loss.

A defence mechanism for a synchronised attack by multiple black hole nodes in a MANET is proposed by JaydipSen et al. The defence mechanism works by making some modification in the typical AODV protocol and it makes use of data routing information (DRI) table along with the stored and current routing table [8]. In the DRI table, the bit 1 represents true and the bit 0 represents false. From field in the DRI table is for routing data packets from the node and through field is for routing data packets through the node. For a node 3 if the entry is 1 0 that means the node 4 has routed packets from node 3 but not routed packets through node 3. Cross checking relies on trustworthy nodes and it will send packets to the trustworthy nodes only. Trustworthy nodes are the nodes through which the data packets have routed previously. If the data packet is not routed previously to the node that will become the suspicious node and the packets will not be routed to the suspicious nodes. On the basis of simulation carried out it is observed that on applying this proposed mechanism a reasonable level of throughput in the network is maintained.

An algorithmic approach for improving the security of AODV protocol is introduced by Rajib Das et al with the ability to detect and remove the black hole nodes in MANET [5]. An additional route is proposed to the intermediate node that send the RREP message to the source node for identifying the route to destination node is exists or not. The proposed approach cannot be applied to identify the multiple black hole attack consists of multiple nodes.

III. BLACK HOLE PROBLEM IN ROUTING PROTOCOL (AODV)

A black hole problem can be defined as mischievous node introducing itself as an intermediary node having shortest path to the destination, instead of forwarding the packets to its neighbours, it drops the routing packets. Figure 1 consists of six nodes A, B, D, E, F and M respectively, in which M is a malicious node. Whenever node A floods an RREQ packet in the network, it will be received by nodes B, D and M. It is known that Node M is a misbehaving node,

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

therefore it sends back a RREP packet instantly on receiving the request and advertising itself having the shortest path to the destination without even consulting its routing tables for the requested route to node *E*. The node A will receive reply from M earlier than any other node in the network. Hence it will assume that M holds the shortest path to the destination & will start transmitting packets to it. Node M will behave like a black hole by absorbing all the packets sent to it.

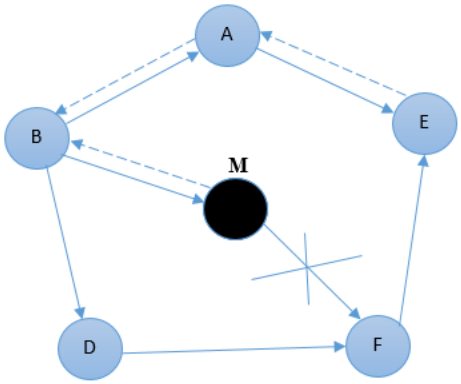

Figure 1 Black Hole Attack

In AODV, the freshness of the routing information obtained from the sequence number present in the routing packets. When a source node broadcasts the RREQ message for desired destination node, if there exist a black hole node in the network then the black hole node as shown in Figure 1will instantly send a RREP as a response of the RREQ having the higher value of sequence number and it will be sent in such a manner that the source will think thank it is coming from the original destination node or from a genuine intermediate node which has fresh enough route to the destination. Source will start transmitting the packets which will be absorb by the malicious node. Hence making destination unreachable.

3.1 Multiple Black Hole Problem in AODV

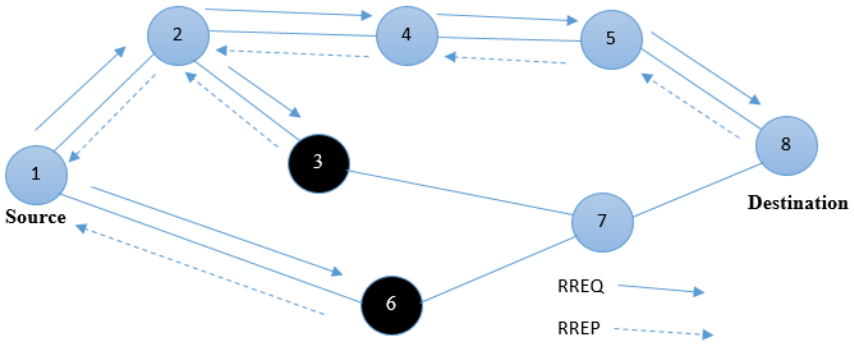

Figure 2 Multiple Black Hole Attack

AODV works on the basis of the on-demand mechanism to create the paths among the nodes by the desired source nodes. AODV manages the paths till it is required for the source nodes. It generates trees to associate with the multiple-cast category branches. The tree consists of the category branches and the nodes should integrate with its members. It is using the sequence number to preserve the originality of paths. In the presence of multiple black hole nodes as displayed in Figure 2, the misbehaving nodes will fabricate a RREP consisting of highest sequence number value, in order to introduce itself having a shortest path to the intended destination. The source node will rely on the information

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

obtained from the RREP and it will start sending packets to that malicious node. A malicious node can be present at any place in the network. In the above figure there are more than one adversary nodes in the network which in our case are node 3 & node 6.

IV. PROPOSED DESIGN

In MANET inside and outside attacks are possible, which degrade the performance of the network. In Inside attacks, a node within the network become malicious node and it launched attacks on the network. In outside attacks, a malicious node which is outside the network, it become the member of the networks and then launched the attack on the network. A passive outsider eavesdrops on all the communication and aims to compromise the privacy. Among all the attacks discussed previous black hole attack is the most common active type of attacks. Black hole attack is the denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been proposed to isolate black hole attacks from the network. When black hole attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. The black hole attack is even worse if there are multiple black hole nodes exist in the network. When multiple black hole nodes exist in the network, all the malicious nodes are responsible for triggering the black hole attack. This type of attack is called multiple black hole attack. In our work, we work on to detect and isolate multiple black hole attack in mobile Ad hoc network.

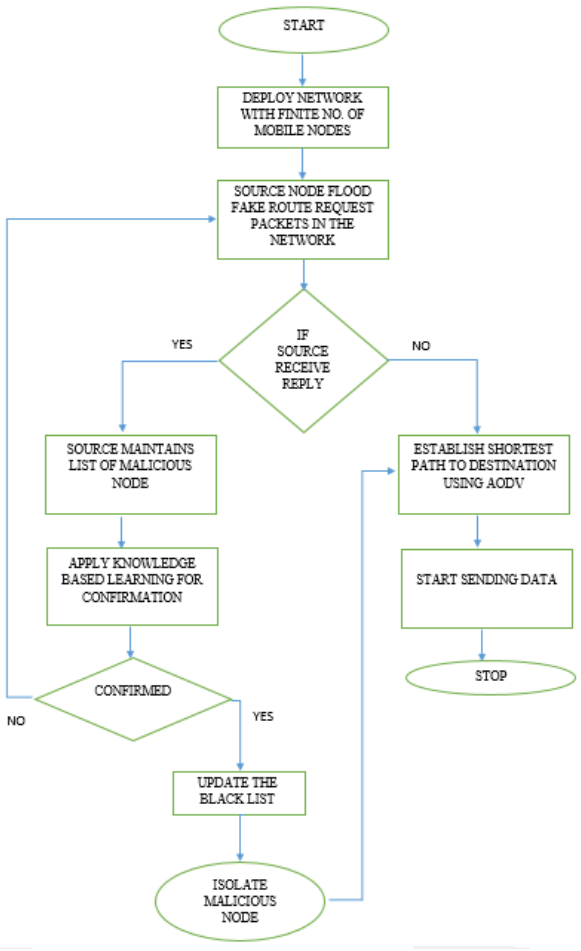

Figure 3 Flowchart of our proposed algorithm

A significant amount of research has been devoted to study security issues as well as countermeasures to various attacks in MANET. However, there is still much research work needed to be done in the area. This paper propose a

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

solution on finding a secure route for the communication by identifying and isolating all the malicious nodes present in mobile Ad hoc network to provide enhanced security and stability to MANET.

In Figure 3, at first the network is deployed with finite number of mobile nodes. Source andDestination are assigned in the network after that the source node broadcast a Fake RouteRequest containing a bogus destination address in the network. In this scenario if there isany black hole node present in the network then it will reply to source's requestwith aRoute Reply Packet (RREP) , on receiving that packet source will add the respondingnode to its black list &then knowledge based learning will be applied for confirmation ofthe malicious node if the node is confirmed beingmalicious then blacklist will be updated & an alarm message will be broadcasted in the network containing the id of the maliciousnode in order to isolate the malicious node and to inform all the nodes present in thenetwork about the existence of the malicious node. After the malicious node is isolated,shortest path will be created with the help of AODV protocol & communication will takeplace. If the malicious node is not confirmed by applying the knowledge based learning then step 3 will be repeated i.e. source will again broadcast a fake route request packet if it doesn't receive areply then the normal route discovery process using AODV protocolwill take place & shortest path will be established tothe destination. The communicationwill take place on the established path.

V. PERFORMANCE EVALUATION

1. Simulation Configuration:

The simulation for the proposed method has been carried out using the network simulator 2 &graphical interface is created using network animator and the operating system used is Ubuntu 14.0.4. The network animator shows the positions of various nodes. The operating system used is installed on Virtual box which is allocated 4 GB RAM, 30 GB HDD and Intel 2.2 GHz Quad core Processor.

In our simulation we are creating a network consisting of 15 nodes, the protocol used is AODV, number of malicious node in the network are 2and the graphs of the results are generated using reference node technique.The graphs are used to signify the variation in throughput, packet loss and end-to-end delay using the proposed method. Green line characterizes the change in case of the new scenario and red colour represents the conventional method.

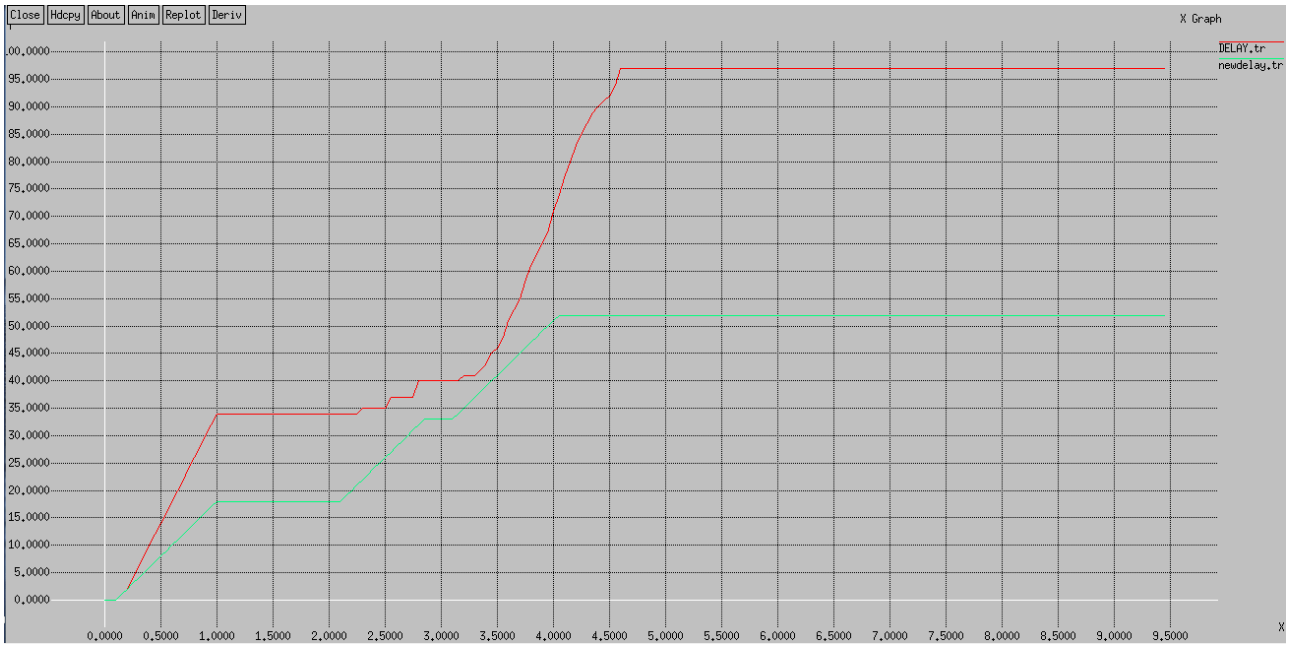

Figure 4 End-to-end delay

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

These two parameters are a widely used for validating and confirming the use of particular methods.Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination. Figure 4 shows the change in end-to end delay after the deployment of the proposed method. It shows that the proposed method reduces the end-to-end delay while packet is going to transmit from source to destination. In the previous schema, the delay starts linearly increasing when there is a presence of malicious node in the path mark as red line whereas in absence of malicious node delay first decrease but the new path deploy because of malicious activity it will be not as much shortest then previous so at some point of time the peak of the graph increase and decrease because of delay which mark as green line in graph.

Figure 5 represents the network throughput after applying proposed method. As delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increased after some pint of time. From the graph, we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by green line. While red line represents previous schema when the malicious node present in the network at that time packet continuous drop so the line is constant for some period of time.

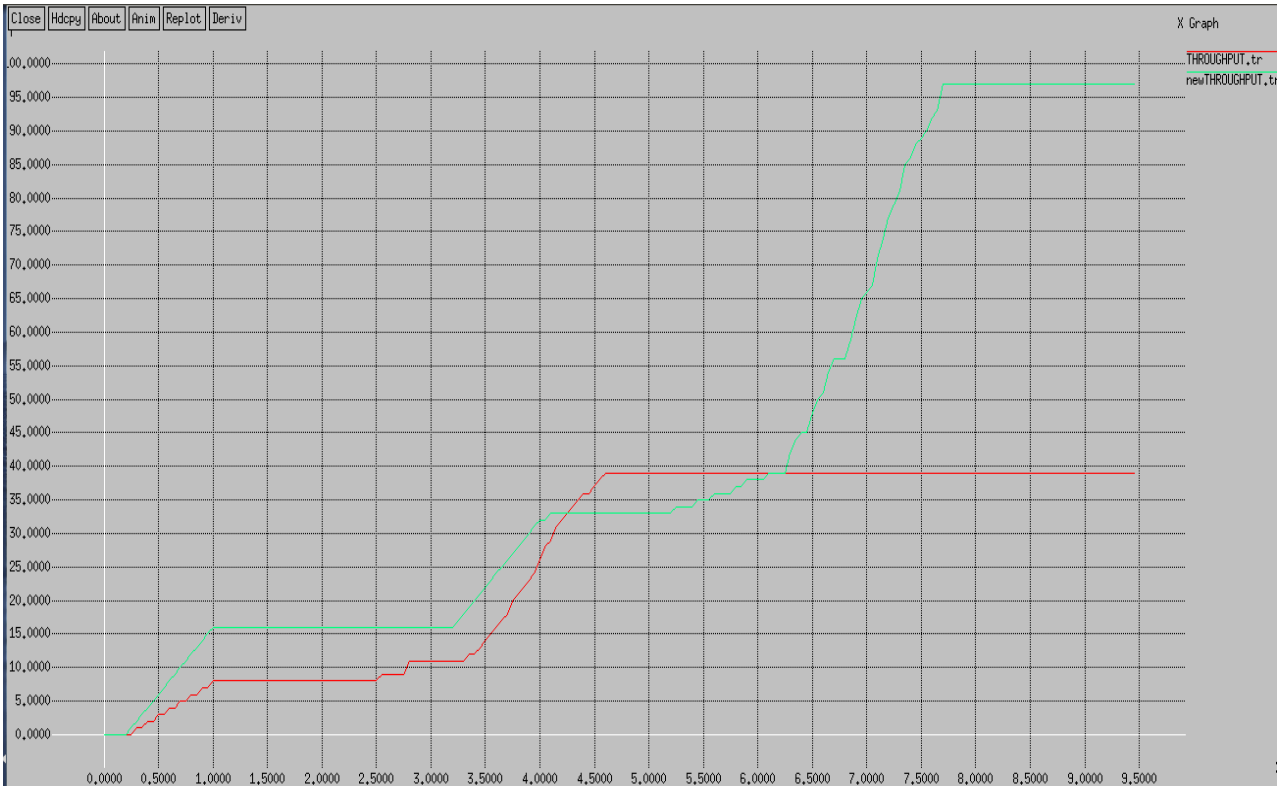

Figure 5 Throughput

As we have applied the proposed algorithm for setting up the path then packet loss is less as compared to the previous scenario. We make the channel secure so final result comes is the maximization of throughput and minimization of packet loss. In previous schema malicious node continuously dropping the packet so final output is major loss of packet. In Figure 6 we see that the red line is continuously increase because of dropping of the packet and green line constant after some time because of securing of channel.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

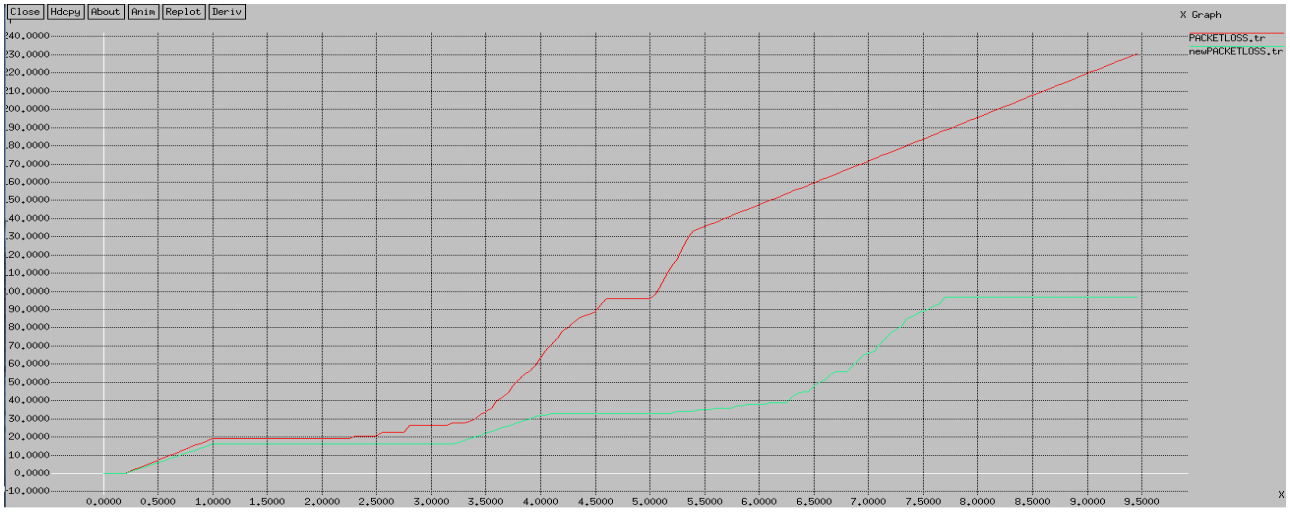

Figure 6 Packet Loss

VI. CONCLUSION

As MANET being infrastructure less it can be deployed with fewer efforts as compared with the traditional network infrastructure environment. It has a lot of potential but still there are some issues to overcome. One of the popular research areas nowadays is security in MANET and in our thesis we are addressing security issues in one of the reactive routing protocol (AODV) in MANET. In earlier research conducted, solutions introduced are lacking in terms of effectiveness or efficiency. If any proposed algorithm works in presence of a black hole attack then there are chances that it will not work under multiple black hole attack. The algorithm proposed by us can work effectively & efficiently in both the scenarios of a single as well as multiple black hole attack. Our future task will be to develop an algorithm which is capable in detecting the above mentioned attacks as well as collaborative black hole attacks in which nodes act in coordination with each other and are successful in evading detection.

REFERENCES

[1] Latha Tamilselvan and V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", JOURNAL OF NETWORKS, VOL. 3, NO. 5, 2008.
[2] Mohammad Al-Shurman and Seong-Moo Yoo "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, 2004.
[3] Priyanka Goyal, Vinti Parmar and Rahul Rishi3 "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering &Management, Vol. 11, 2011.
[4] Durgesh Wadbude and Vineet Richariya "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012
[5] Rajib Das, Bipul Syam Purkayastha and Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach",International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4, 2011.
[6] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003.
[7] Yibeltal Fantahun Alem and Zhao Cheng Xuan "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication, 2010.
[8] Jaydip Sen, Sripad Koilakonda and Arijit Ukil "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", 2011.
[9] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks", Computing and Information Sciences, 2011.
[10] Kitisak Osathanunkul and Ning Zhang "A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks", 2011 International Conference on Networking, Sensing and Control Delft, the Netherlands, 2011.
[11] Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security, 2009.
[12] Sheenu Sharma, Roopam Gupta "SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS", Journal of Engineering Science and Technology Vol. 4, No. 2, pp. 243 – 250, 2009.
[13] S.Sankara Narayanan and S.Radhakrishnan , "Secure AODV to Combat Black Hole Attack in MANET" , International Conference on Recent Trends in Information Technology (ICRTIT), 2013.