Detection and Mitigation of Black Holes in MANET

Ridhi Chawla[1] Pankaj Kapoor[2]
[1]Student, Department of Computer Science & Engineering
[2]Asstt. Prof. Department of Computer Science & Engineering
[1, 2] Kurukshetra University. SIET, Aliyaspur, Haryana, India,

Abstract—A Mobile Ad Hoc network (MANET) has emerged as an important technology of the present world because of the increase in demands of the wireless techniques. It is an infrastructure less network because of this characteristic it is more prone to the outside attacks which harm the security of the network/ there are many kind of attacks which effect the security of the MANET. In this paper we discussed one of the most common type of attack that is known as BlackHole Attack. The node which is responsible for such type of attack is called black hole which prevents the efficient transfer of data in a network. The Modified Ad Hoc On Demand (AODV) protocol approach have been used to detect and mitigate the black hole problem. Simulation Results have been explained in terms of Packets lost and received, End to End Delay. Experiments have been performed by using Network Simulator 2 to verify our results.

Keywords:-MANET, AODV, Black Hole, RREQ, RREP, RRER

I. Introduction

A. *Manet*

MANET(Mobile Ad hoc Network) is a type of network where mobile nodes communicate over wireless channel. The standard protocols used by MANET such as Ad Hoc On Demand(AODV),Dynamic Source Routing(DSR) etc. are designed with less security constraints, as a result these protocols are prone to attacks such as Blackhole attack ,Warm hole attack, Jamming, Snooping etc. MANET is characterized by its Self positioning and Self managing nature and it offers special benefits to the networks where there is no fixed infrastructure. It basically uses two types of protocols that is Proactive(table driven) and Reactive (on demand) protocols. When there is demand for both the protocols simultaneously then hybrid approach is used which has features of both proactive and reactive protocol. MANETs offer wide applications in Commercial & Civilian Environment, Education, E-commerce, Business, Emergency, Military fields etc.

B. Ad Hoc On Demand (AODV) Protocol: AODV is a reactive or On Demand Protocol .It is called On Demand protocol because it does not initiate route discovery by itself until it is requested by as source node. So this type of Protocol is source initiated protocol. These donot consume bandwidth everytime, only when data gets transmitted from source to destination then the bandwidth gets consumed

C. AODV uses three types of control Messages:

1) Route Request (RREQ): When a source node wants to communicate with another node in the network it sends RREQ message. The Time To Live(TTL) value is associated with every RREQ message which states the number of hops the RREQ should transmit.

2) Route Reply (RREP): Whenever there is a node that has requested identity or has route to the requested node generates an RREP message and send it back to the source or originator node.

3) Route Error (RRER): Every node in the network plays its role by maintaining the link between the nodes during active routes. Whenever any link gets broken then an RRER is generated by the nearby node to inform that the link is broken.

Route Discovery in AODV

As the AODV is source initiated protocol so there is a discovery of the route. The route discovery process in AODV can be well explained as below:

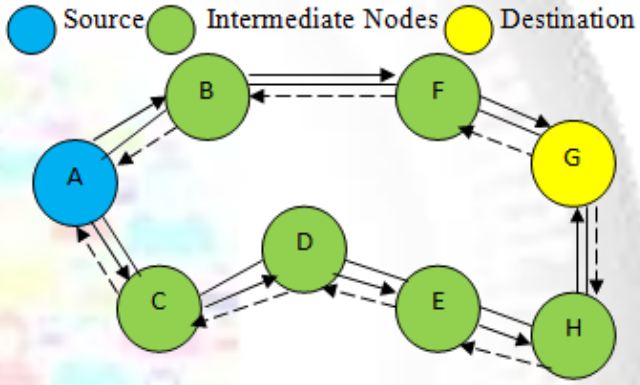

Fig. 1:*RREQ and RREP messages*

In Figure 1 A is the source node and G is the destination node. A wants to discover a route to G so it broadcasts RREQ message which travels through the intermediate nodes B,C,D,E,F,H. These intermediate nodes send RREP messages in Reply to the source node A.

RREQ Message
RREP Message

RREP messages are sent by the nodes only when they have a route from source to the destination.

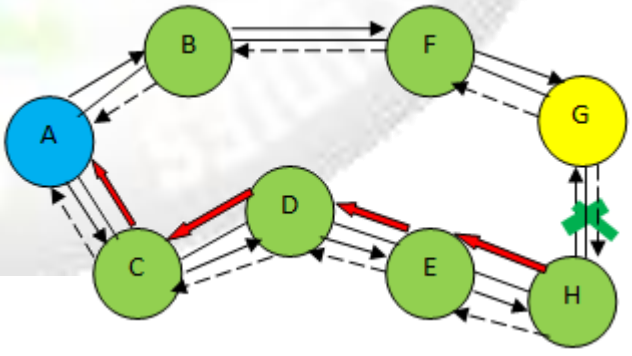

Fig. 2:*RRER messages*

When any link is broken between any intermediate node and destination then that node sends RRER message to the source node in order to notify that error has occurred or link is broken.

RRER Message

Link Broken

In Figure 2 the link is broken between the node H and the destination Node G so H sends RRER message so that sender can be notified about the breakage of the link between the node H and destination G.

4) Black Hole: A black hole is a malicious node in a network which results into black hole attack problem in a MANET. It is kind of Denial of Service(Dos) attack. It is a node which drops the packets during the time of route discovery in a Network. When a source initiates the route the black hole node present in the network sends false message to the Source node or any intermediate nodes notifying the route to destination. But actually it does not have any route to the destination node .When a blackhole receives a packet it drops it and does not forward it to the destination. Thus it results into the black hole attack in the MANET. This is one of the most common security threat of the MANET.

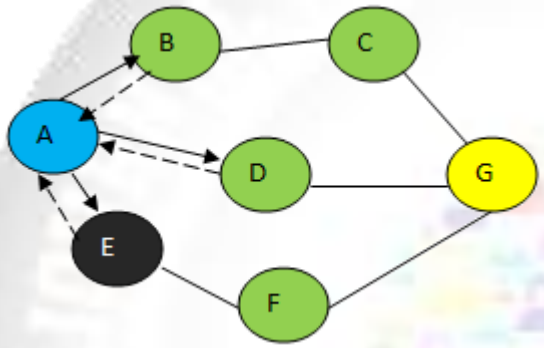

Fig. 3: Black Hole Attack

In Figure 3 let us imagine that E is a black hole.When node A broadcasts RREQ message, the node B,D,E receive the message. Node E does not check its routing table for route to the destination G and immediately sends RREP message to the source node. The source node A after receiving the RREP message sends the packet to Node E assuming that the shortest path exists from E to G. When node E receives the data it absorbs all the data and behaves as a black hole and does not forward the data to the node G.

II. Related Work

Many proposals have been suggested regarding the detection or avoidance of the black hole attacks in MANET. Some of them are:

In[1] Ramasamy Mariappan et al. Proposed a scheme like Re-Pro Routing Protocol in wireless Mobile Ad Hoc Network and described a comparative performance for protocols like AODV focusing on the effect of changing the number of receivers and increasing the number of nodes. Their scheme included a mechanism dependent on Electronic Code(EC) with permutation functions. The results were shown in terms of low time complexity, Easy implementation, Inexpensive and very high brute force It takes time for a trust to grow therefore EC was used.

In [2] Sanjay K. Dhurandher et al. proposed an Efficient Reactive and Angular –Optimized Link State Routing Protocol(ERA-OLSR).ERA-OLSR omits use of routing table from OLSR and next hop decided by angular concept. ERA-OLSR was compared to the well established protocols such as AODV and DSR. The results that were achieved were better performance in terms of End to End Delay & Average Energy Consumption.

In[3] Shobha. K.R. et al. proposed a scheme in which an enhancement of DSR protocol was performed by using combination of Flooding and Relay Routing. Flooding when used alone causes routing overhead therefore relay routing with flooding was used. Relay routing selects small number of nodes in neighbourhood for route discover and route maintenance. Selection was performed on the basis of mobility of neighbourhood nodes at that instant of time.

In [4] Prashant Dewan et al. proposed a reputation scheme. Instead of choosing a shortest path, source chooses a path whose next hop has highest reputation. In this scheme the throughput got increased to 65% from 22%.Improvement was achieved at the cost of high number of route discoveries with minimal increase in average hop length.

In[5] Krishna Paul et al. Proposed a model to discourage selfish nodes from performing the attacks that are sophisticated in civilian co-operation based ad hoc networks. In this paper a large range of attacks on DSR have been detected &and originator of the attack also been detected. This scheme provided a way to inform other nodes of the system about accused and malicious accuser without doubt.

In [6]Hidehisa Nakayam et al. Proposed a new anomaly detection scheme based on dynamic learning process that allowed training data to be updated at particular time intervals. Calculation of Projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve was done. Effective results in terms of high delivery ratio and low False Positive Rate against five simulated attacks were achieved.

In]7] IssacWoungang et al. Proposed a scheme named as DBA-DSR scheme for detecting and avoiding black holes. The scheme started by using fake RREQ packets to catch malicious nodes. Network throughput and packet delivery ratio were chosen as performance metrices. Proposed scheme worked better than DSR scheme in terms of network troughput and minimum packet loss.

In[8]N.Bhalaji et al. Proposed Association based(AB) DSR protocol. For analysing the performance three parameters named as Packet Delivery Ratio, Throughput and percentage of dropped packets were worked upon. The Throughput and packet delivery ratio were high and total black holes dropped were less because no malicious nodes were present in AB-DSR

III. Proposed Detection And Mitigation Scheme

The scheme proposed in our work for the detection and mitigation of black holes in MANET works as follows:

1. The source node periodically requests one of the backbone nodes for a restricted IP address. Whenever the node wants to make a transmission.
2. After confirmation of RIP the source node sends packets to all the intermediate nodes.
3. If the RIP is not available then dummy packets are sent to the intermediate nodes and packet loss is checked if it is greater than the threshold value the node is added to the blacklist.

The proposed Modified AODV scheme will be compared to existing AODV scheme in terms of two

parameters such as Packets Lost and Received and End to End Delay.

IV. PERFORMANCE EVALUATION

Network Simulator 2 has been used as the simulation tool to carry out the proposed method for detecting and mitigating the black holes.

We have taken total of four nodes and eight nodes in our simulation evaluation process as shown in the following figures.

*A. Four Nodes Network:*In Figure 4,5,6,7 we have a network of four nodes communicating with each other with time.

- The black circles indicate the nodes
- The blue circles indicate the duplex links between the nodes.
- The blue dots indicate the balck hole packets being dropped.

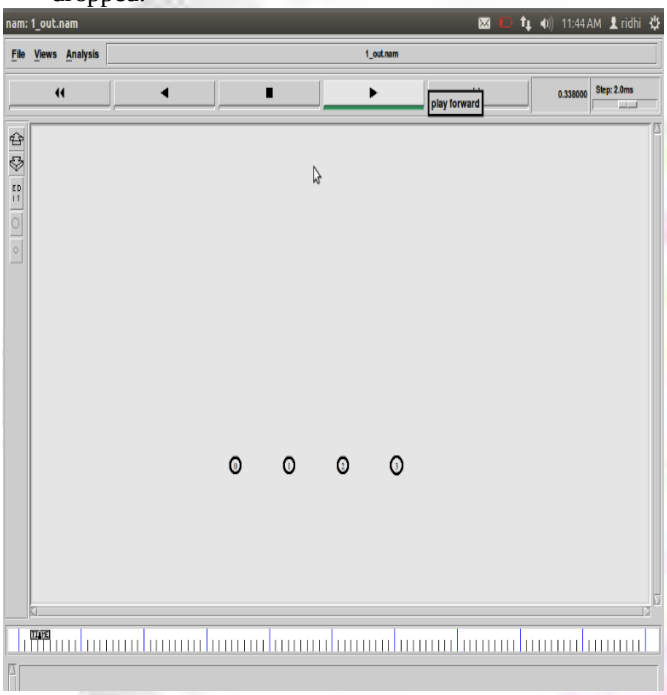

Fig. 4:Initial States of mobile nodes

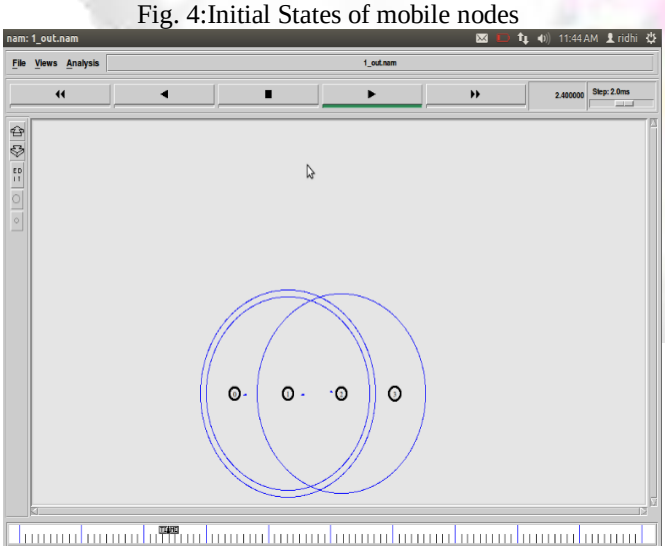

Fig. 5: Communication between nodes 0 and 3 via node1 and 2

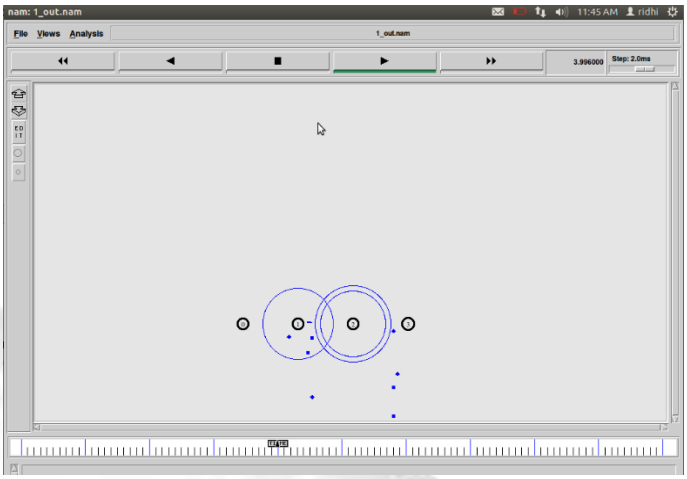

Fig. 6:Black hole packets dropping

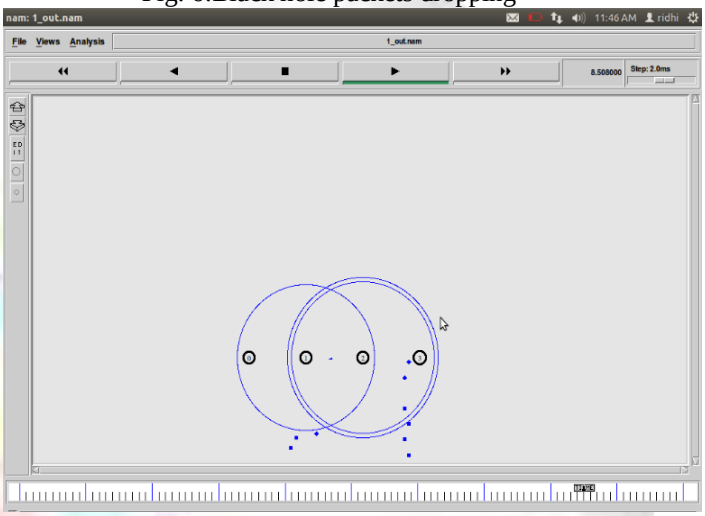

Fig. 7:Black hole packets dropping continued with time

B. ***Eight Nodes Network:*** *In Figure 8,9,10,11,12 we have a network of eight nodes communicating with each other with time.*

- The black circles indicate the nodes.
- The blue circles indicate the duplex links between the nodes.
- The blue dots indicate the balck hole packets being dropped.

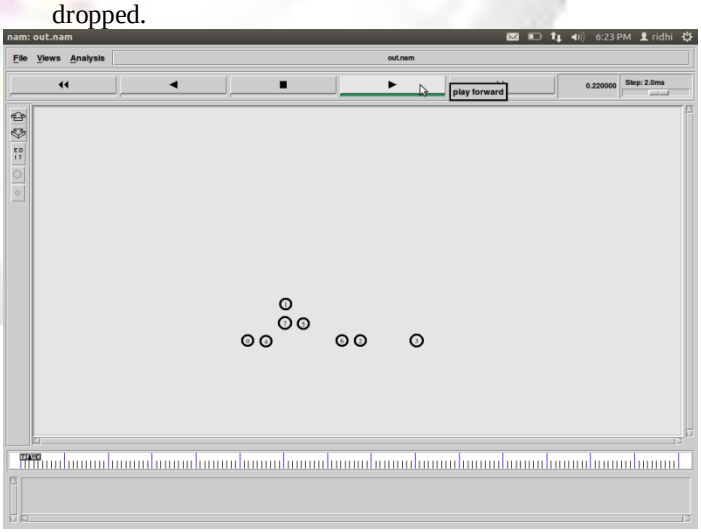

Fig 8:Initial states of mobile nodes

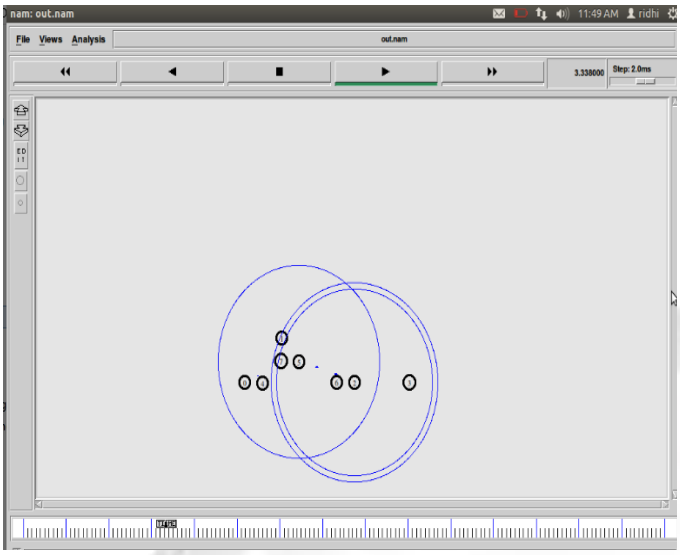

Fig. 9:Communication between nodes via duplex links

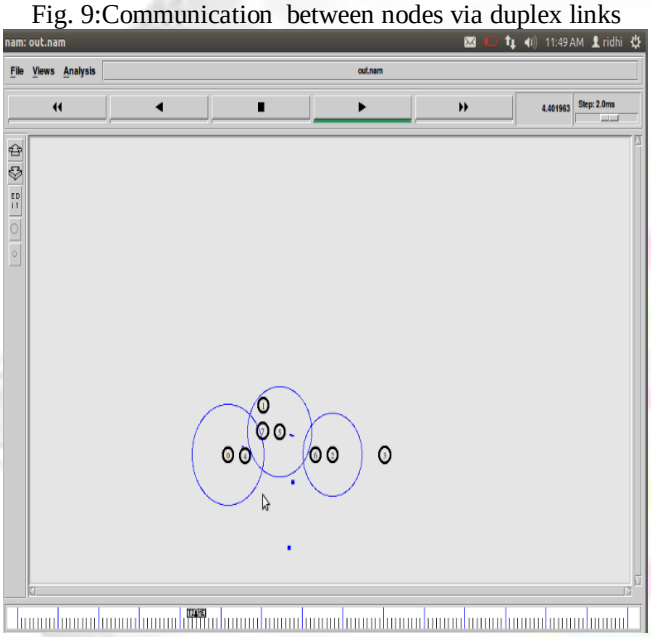

Fig. 10:Black hole packets dropping started

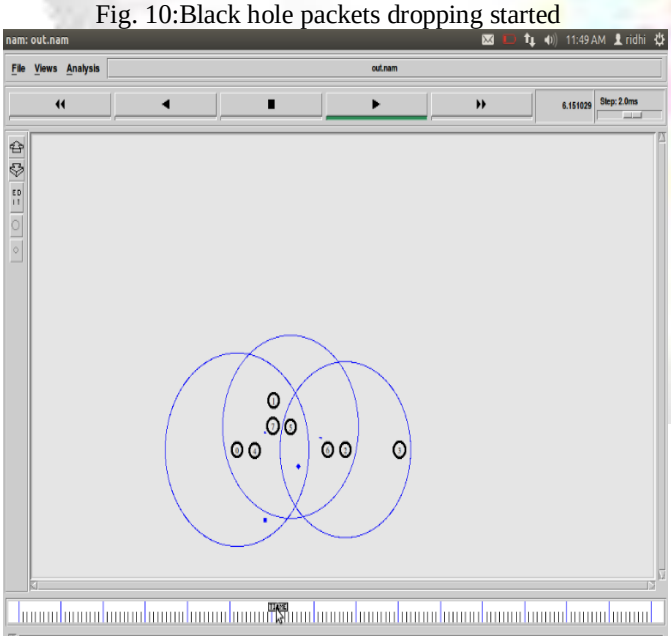

Fig. 11:Black hole packets dropping continued

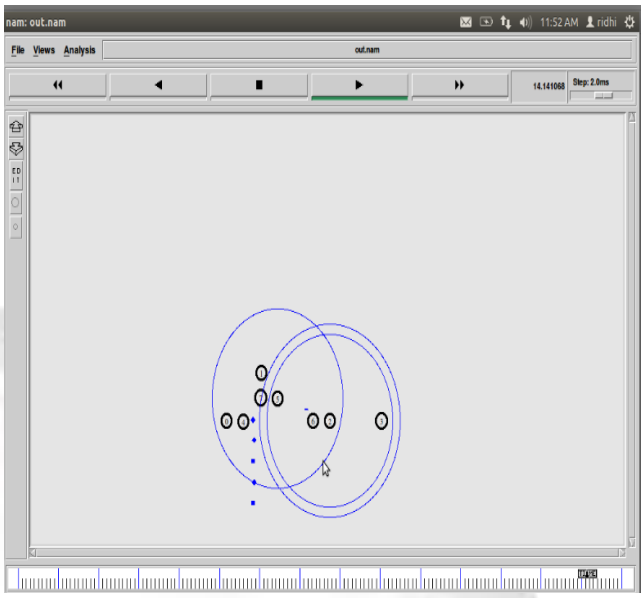

Fig. 12:Black hole packets dropping reaching the end

V. SIMULATION RESULTS

A. Parameters analysed in Four nodes network:

(a)Packets Received and Lost
(b)End to End Delay
The simulation was performed for 10 seconds.

B. Four Nodes Network Results :

(a) Packets Received and Lost

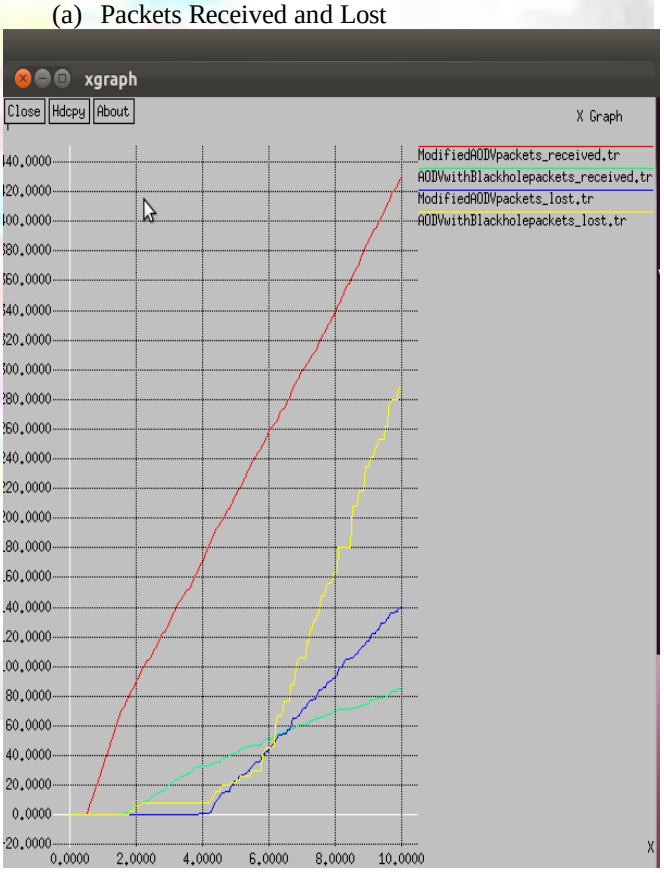

Fig. 13:Xgraph for comparison of AODV Black hole Packets Recieved and Lost with Modified AODV Black Hole Packets Received and Lost

- The Green line in the graph is indicating the AODV Black Hole Packets Received
- The Red line in the graph is indicating the Modified AODV Black Hole Packets Received
- The Yellow line in the graph is indicating the AODV Black Hole Packets lost
- The Blue line in the graph is indicating the Modified AODV Black Hole Packets lost

(b) End To End Delay

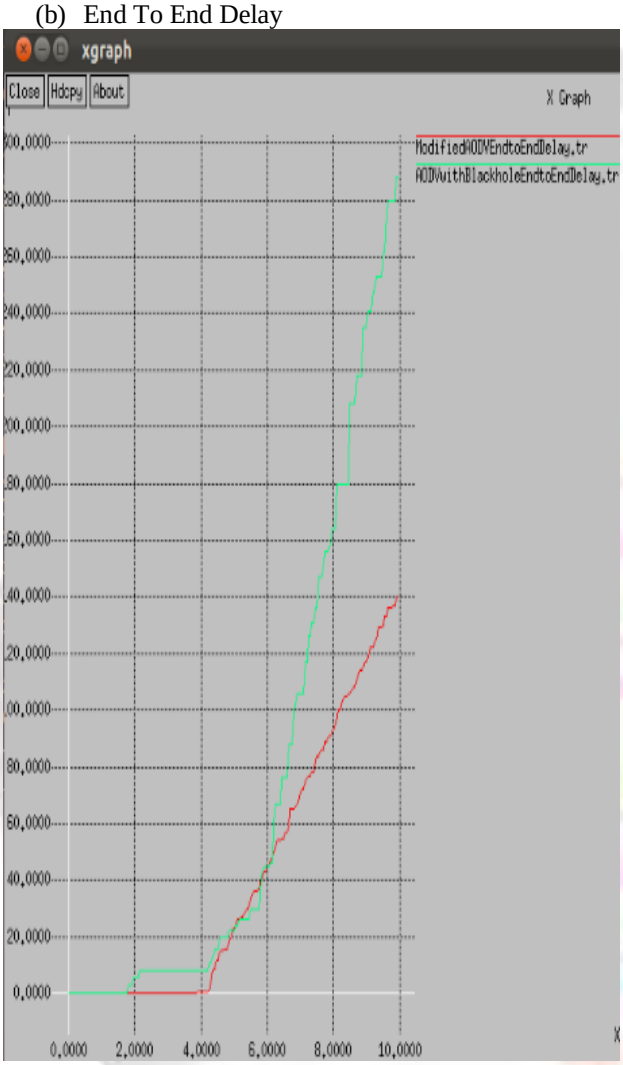

Fig. 14:Xgraph for comaparison of AODV Black hole Packets End To End Delay with Modified AODV Black Hole Packets End To End Delay

- The Green line in the graph is indicating the AODV Black Hole End to End Delay
- The Red line in the graph is indicating the Modified AODV Black Hole End to End Delay

C. Parameters analysed in Eight nodes network:

(a) End to End Delay

The simulation was performed for 15 seconds

D. Eight Nodes Network Results :

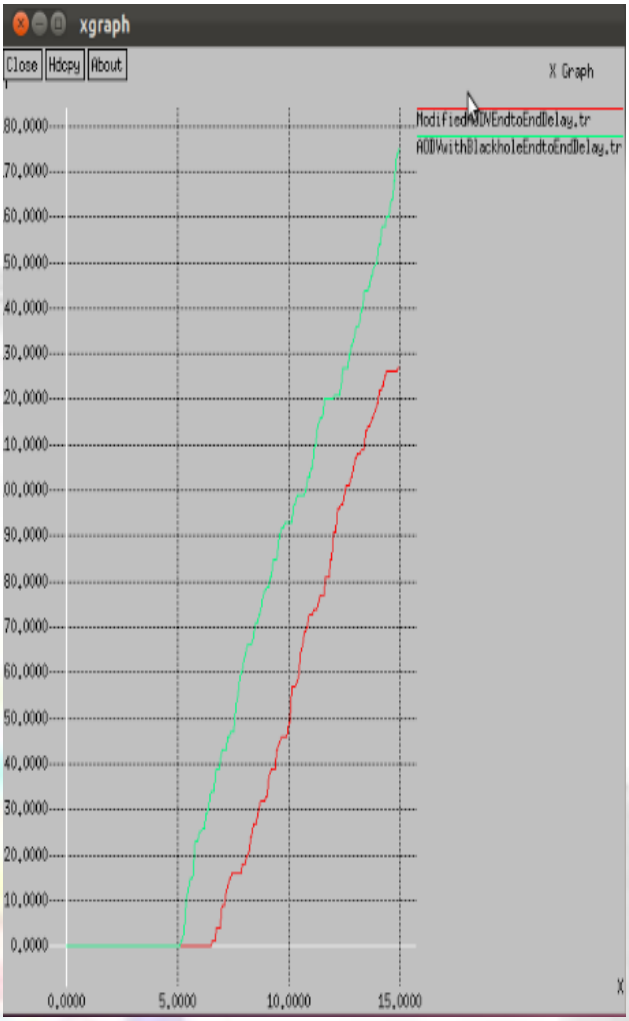

Fig. 15:Xgraph for comaparison of AODV Black hole Packets End To End Delay with Modified AODV Black Hole Packets End To End Delay

- The Green line in the graph is indicating the AODV Black Hole End to End Delay
- The Red line in the graph is indicating the Modified AODV Black Hole End to End Delay

VI. Conclusion

In this paper we proposed the modified AODV scheme which is a solution to practicable AODV solution to detect and mitigate the black holes in MANET. The Simulations results achieved proved that original AODV suffers from Black holes to a large while considering the packets Received and Lost and End to End delay. The proposed modified AODV Performed better than AODV scheme in terms of the parameters mentioned. In future we plan to expand the proposed Modified AODV Scheme by performing simulation on the parameters such as throughput, Network overhead to minimize and remove black hole attacks.

References

[1] Ramasamy Mariappan Sangameswaran Mohan “Re-Pro Routing Protocol with Trust Based Security for Broadcasting in Mobile Ad hoc Network”,2012

[2] Sanjay K. Dhurandher, Mohammad S. Obaidat, Mukta Gupta "A Reactive Optimized Link State Routing Protocol for Mobile Ad hoc Networks",2010
[3] Shobha. K. R , Dr. K. Rajanikanth "Efficient Flooding Using Relay Routing in On-Demand Routing Protocol for Mobile Adhoc Networks",2009
[4] Prashant Dewan, Partha Dasgupta and AmiyaBhattacharya"On Using Reputations in Ad hoc Networks to Counter Malicious Nodes"
[5] Krishna Paul,DirkWesthoff"Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks",2002
[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto and NeiKato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" IEEE Transactions on Vehicular Technology, Vol. 58, No. 5, JUNE 2009
[7] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat Fellow of IEEE andFellow of SCS, "Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks",2012
[8] N.Bhalaji, Dr. A. Shanmugam "Association between nodes to combat Blackhole attack in DSR based MANET",2009
[9] Lu Han, October 8, 2004 "Wireless Ad-hoc Networks
[10] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester "An Overview of Mobile Ad HocNetworks: Applications and Challenges", Session 4