ISSN:0975-9646

Performance Analysis of Black-Hole Attack in MANET

Jyoti[1], Ms Rashmi Kushwah[2]
[1]*M.Tech. Scholar, P.D.M College of Engineering, Bahadurgarh, Haryana (India)*
[2]*Assistant Professor Of CSE, P .D.M College of Engineering, Bahadurgarh, Haryana (India)*

Abstract: **Data Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. A Mobile ad-hoc network (MANET) is a latest and emerging Research topic among researchers. The reason behind the popularity of MANET is flexibility and independence of network infrastructure. MANET have some unique characteristic like dynamic network topology, limited power and limited bandwidth for communication. MANET has more challenge compare to any other conventional network. The most common routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol. AODV protocol is threatened by "Black Hole" attack. In black hole attack a malicious node advertise itself as having the4 shortest path to the destination node. To combat with black hole attack so many solutions provided by researchers. In this article we study the routing security issue of MANET and analyze in detail one type of attack the "Black hole" attack. We also provide a detailed list of solutions which protect the black hole in MANET's..**

Keywords: **MANET, AODV Routing protocol, Black-hole, NS2**

I.INTRODUCTION

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in MANET" on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

1.1. Black Hole Attack:- In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [1]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig. below shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

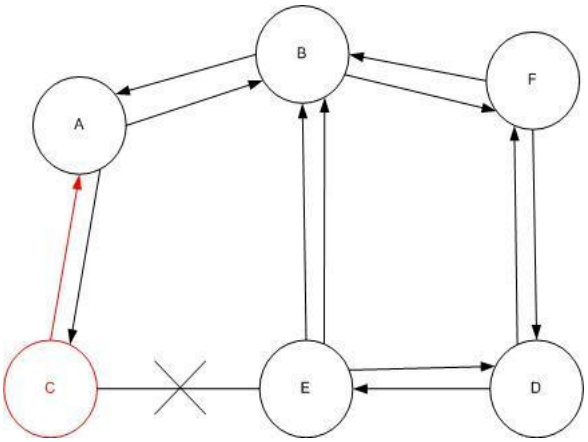

Fig1: black hole problem

1.1.1 Black hole attack in AODV:-

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.[2]

1. Internal Black hole attack:--This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination.

2 External Black hole attacks:-External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network.. External black hole attack can be summarized in following points.

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value

is set to lowest values and the sequence number is set to the highest value.

- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update its routing table.

If the data is not missing at random or informatively missing then it is termed as "Not missing at Random". Such a situation occurs when the missingness mechanism depends on the actual value of missing data. [4].

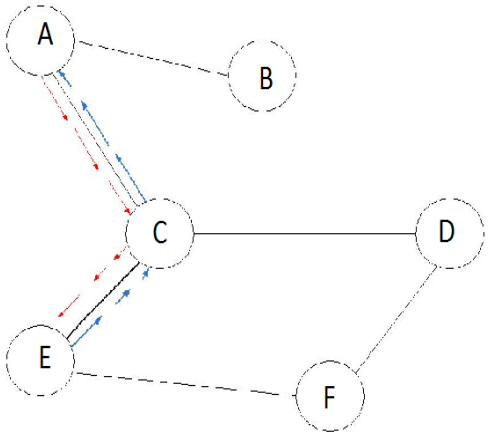

Fig2: black hole attack specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

1.1.2 .Other Attacks on MANET:-

Gray Hole Attack:- In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [2]. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack .

Flooding Attack:- The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [16]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

Selfish Node :-In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption . The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network.The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network.

Wormhole Attack:-Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. They make the use of their location i.e. they have shortest path between the nodes. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network. When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole. The other type of wormhole attack is known as in band wormhole attack . In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

Sleep Deprivation Torture Attack:-One of the most interesting attack in MANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

Jellyfish Attack:-In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network . In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably affect the performance of the network.

Modification Attack:-The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack. Misrouting and impersonation attacks are two types of modification attack.

Message tampering:-An attacker can also modify the messages originating from other nodes before relaying them, if a mechanism for message integrity (i.e. a digest of the payload) is not utilized.

Replay attack:-As topology changes, old control messages, though valid in the past, describe a topology configuration that no longer exists. An attacker can perform a replay attack by recording old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes. This attack is successful even if control messages bear a digest or a digital signature that does not include a timestamp.

Rushing attack: -An offensive that can be carried out against on-demand routing protocols is the rushing attack. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.

Misrouting Attack :-In misrouting attack a malicious node which is part of the network, tries to reroute the traffic from their originating nodes to an unknown and wrong destination node. As long as the packets remain in the network make use of resources of the network. When the packet does not find its destination the network drops the packet.

Impersonation Attack :-In Ad-Hoc networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. In MANETs IP and MAC address uniquely identifies the host. These measurements are not enough to authenticate sender. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack .

Routing Table Overflow Attack:-

Routing Table Overflow attack is usually done against proactive protocols. In this attack, non-existent node data is sent in the network, more ever corrupting and degrading the rate, when routing tables are updated. Proactive routing protocols updates route periodically before even they are required. This is one of the flaws that make proactive protocols vulnerable to the routing table attack. The attacker tries to create so many routes to nodes that do not exist in the network. This is done by using RREQ messages. The attacker sends RREQ messages in the network to non-existent nodes. The nodes under attack results its routing table full and doesn't have any more entry to create new. In other words the routing tables of the attacked nodes are overflow with so many route entries.

II. RESEARCH BACKGROUND

Rahul Sharma1, Naveen Dahiya2, Divya Upadhyay3 Computer Science & Engineering, Amity University, and Noida, India:-proposed a solution with the enhancement of the AODV Protocol which avoids multiple black holes in the group. A technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated.

Hesiri Weerasinghe proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the S.Ramaswamy to improve the accuracy. Rahul Sharma et al, International Journal of Computer Science and Mobile Computing :-Multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). Most of the papers have addressed the black hole problem on the protocol such as AODV

Payal N. Raj, Prashant B. Swadas proposed "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET" (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which

a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated. Their solution increases the average end to end delay and normalized routing overhead.

Zhao Min et.al has proposed a cryptographic based solution (ZHAO), that is, an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function and Message Authentication Code (MAC) which is used for checking the RREPs at source node to send the data packets. The proposed mechanism eliminates the need for a PKI (Public Key Infrastructure) or other forms of authentication infrastructure, however it needs to be discussed, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot forge a reply if the hash key of any nodes to be disclosed to all nodes. This solution consumes much of the computation power of the MANET nodes. [3]

Mohammad Al-Shurman has proposed solution in which host node sends a packet that includes the packet id and sequence number to destination node through three different paths. When any intermediate node or malicious node has a route to the destination Node will reply to that packet. Once the source node collects all the reply from the intermediate nodes, source node will check for the secure route to the destination.

Sanjay Ramaswamy proposed a solution for multiple black hole nodes in a network. He modified AODV routing protocol by introducing new concept of data routing information table and cross checking. In DRI table, every intermediate node maintains a DRI table which will record information about the node traversed before and node traversed after the intermediate node. Once the data is transmitted cross checking is done to check the data loss occurred during the transmission.

Hesiri Weerasinghe:-studied the problem of node to receive route request from the intermediate nodes. Second step is of storing the RREQ destination sequence number (DSN) and node ID into a table called RR table (Route Reply). Next third step is of identifying and removing the malicious node. The first entry in the RR table with the greatest DSN is of malicious node. If the difference between the DSN of source node and the first entry in RR table is much greater than remove that first entry from the RR table. In this way a malicious node is identified and removed. In next step, second entry with higher DSN in the RR table is selected. In the last step, with that entry the default process is continued. Dinesh analysed the behaviour of malicious node in different routing protocols in MANET. He proposed a solution for finding a safe route by waiting and checking the replies received from the intermediate nodes. He observed the network under varying network mobility with maximum speed of 10m/s. He concluded that AODV routing protocol results in a better performance with black hole nodes than DSR in terms of throughput.

Harmandeep Singh1, Manpreeet Singh2 1Research Scholar, Department of IT, GNDEC, Ludhiana, INDIA:- have analyzed the Black hole attack on AODV, OLSR and ZRP with respect to different performance parameters such as Average end-to-end delay, throughput and packet delivery ratio. We conclude the effect of black hole attack is more on AODV protocol as compared to others. In future work we can implement some security algorithm on these protocols to avoid the black hole attack.

Swati Jain1, Naveen Hemrajani2 M.Tech Scholar, Department Of Computer Science & Engineering:- proposed a method for black hole attack prevention. A watchdog method is introduced in the network to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe the neighboring node and decide whether it is a trusted node or a malicious node.

Neighborhood-based and Routing Recovery Scheme Sun et al [4] gave a general approach for the detection of the black hole attack. The method given by them is neighbor based, which detect the malicious node and a routing recovery protocol to establish a correct path to the truthful destination. For this such nodes which within the transmission range of a node forms neighboring node set. The control packets are used to share neighbor set with the other nodes. If two set received at same time and contains different elements, concludes the set generation by two different nodes.

Signature Algorithm - Gao et al [5] projected a signature algorithm to trace packet dropping nodes. The proposal consisted of algorithms to create proof, checkup algorithm and diagnosis algorithm

Time-based Threshold Detection Scheme [6] Latha Tamilselvan et al. propose a solution based a timer approach. A timer is started when first request is received and remain active while the other request from other nodes are collected. It will store the packet's sequence number and received time and count the timeout value based on arriving time of first route request and analyzes the route belong to valid or not based on the threshold value.

Intrusion Detection System based on Anti-black hole mechanism [7] :-Ming-Yang Su proposes an IDS scheme to remove the black hole attacks in MANET The ABM employs two tables called RQ table and SN table The IDS work on the irregular difference between routing information transmitted from a suspicious node. If the value goes beyond the threshold value.It is considered as black hole.

III. CONCEPTUAL FRAME WORK

A. Insert the black hole nodes in Coding of AODV routing protocol:-

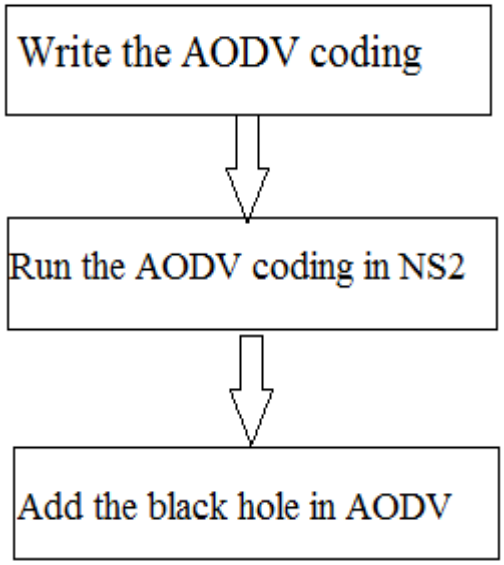

Fig. 3 Diagrammatical representation of problem 1.

B. 2ND Step is to simulate the behavior of black hole attacks using NS2 simulator [8]:- As the name indicates the NS2 is the simulator which was developed for the simulation of the various kinds of the networks, their routing mechanisms, routing protocols, wireless, wired networks, wi-fi networks etc. NS2 is nothing but the discrete event simulator along with the functionality of objects oriented concepts. NS2 [9]was developed in the UC Berkely. The languages such as C++ were used for the development of NS2 simulator In order to shows the simulation of the black hole attacks, we have to use the modified AODV protocol which is simulating different types of misbehaving nodes such as malicious, selfish NODES. From the simulation results, we have aim to find out the detection of the black hole attack or misbehaving nodes from the network and on the detection of it prevention mechanism for it.

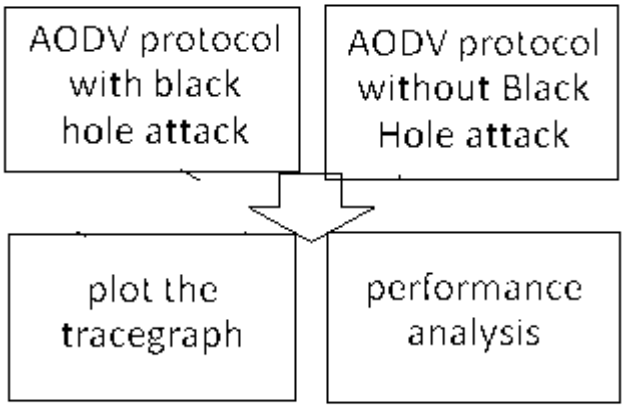

Fig. 4 Diagrammatical representation of problem 2

IV. RESULT AND ANALYSIS

1.) Write the code in gedit editor and save file with .tcl extension and run the file using ns2 as

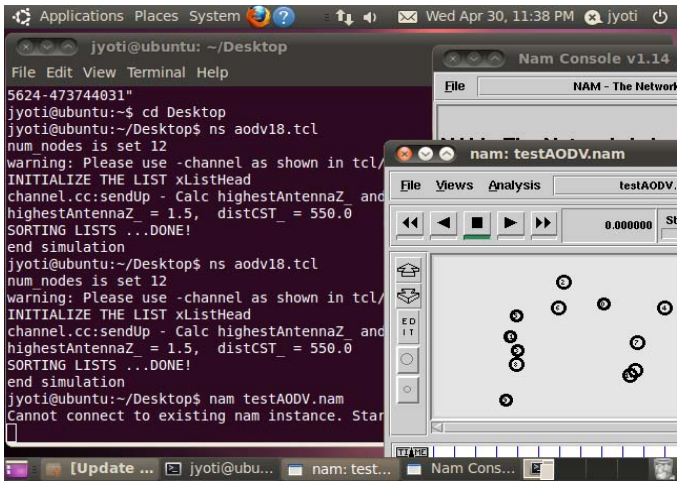

Fig5: running .nam file

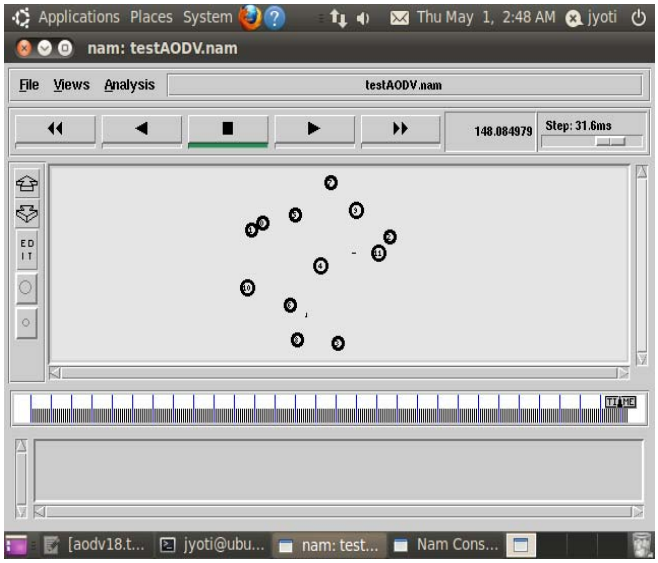

Fig6: sending data from node 2 to 11

2) Adding the blackhole node in AODV:-

Set node 5 as malicious or black hole node:- Here we are adding a malicious or black hole node in the aodv.tcl file which we have already seen. We are inserting or making the node 5 as a black hole node here. We can make any node as malicious node also we can create multiple black hole nodes within one .tcl file. But here we are dealing with only detection of single black hole node problem, so not more than one node is made malicious here.

Do some changes in files - we have already change the .tcl file , so the new file with malicious node will not work well until we modify the aodv.h and aodv.cc

3) simulation after adding malicious node:- node 5 has larger distance form destination than other but still he accepts the packet from source node acting as nearest node to destination. As shown below :-

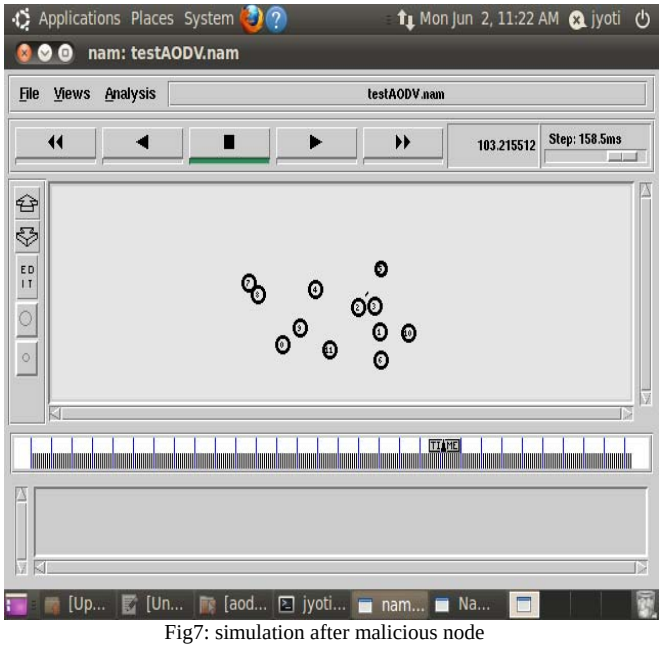

Fig7: simulation after malicious node

4. Performance Analysis :-

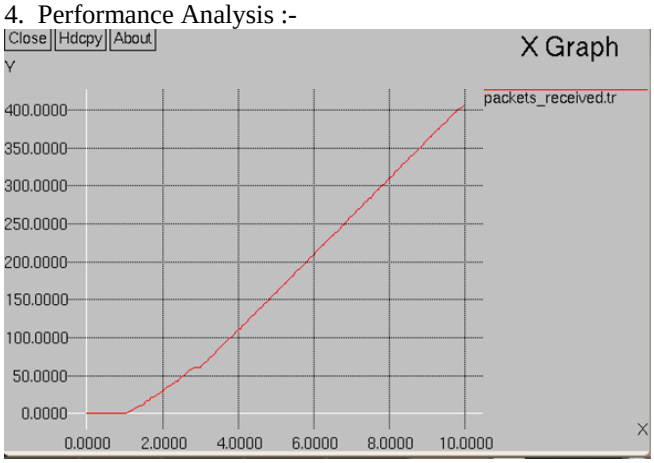

Fig.8: Packet Received

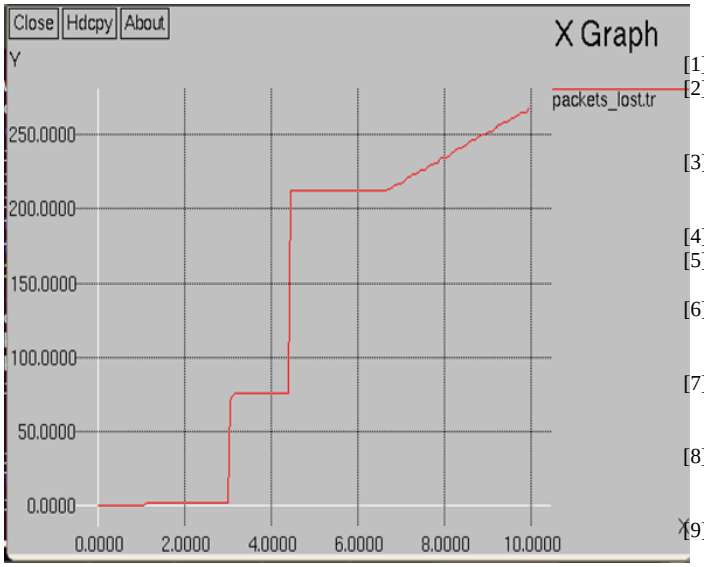

Fig9: Packet lost

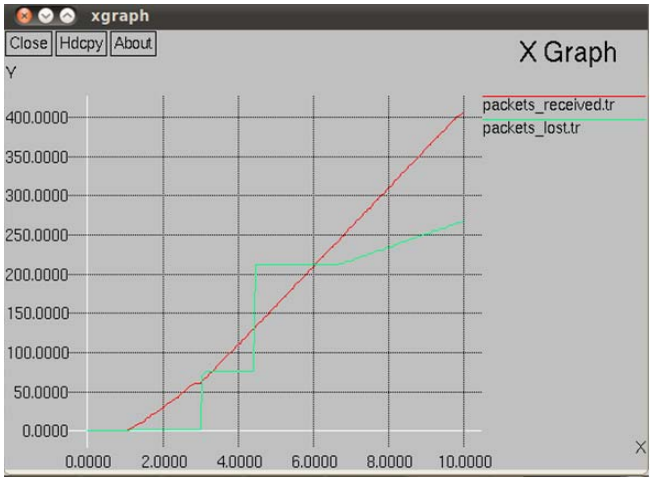

Fig10: Comparision of received and lost packets

V. CONCLUSIONS

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique.Here we use the AODV and using the modified protocol, we can detect the Black hole attack in MANETs. We have proposed a feasible solution for the black hole attacks that can be implemented on the modified AODV protocol. These Proposed methods can be used to find the secured routes and prevent the black hole nodes in the MANET. save our network when a number of malicious nodes attack network at same time.

ACKNOWLEDGMENTS

Author would like to thanks to her head Ms Rahmi Kushwah, Asst. Professor of CSE & I.T department, PDMCE, Bahadurgarh for their valuable support and help

REFERENCES

[1] http://www.techterms.com/definition/manet
[2]http://www.bth.se/fou/cuppsats.nsf/all/448194ba63f382fdc1257751006226b8/$file/Final_Thesis_Report_irua08_resa08%20Analysis%20of%20Blackhole%20Attack.pdf
[3] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007
[4] http://www.ijcsmc.com/docs/papers/April2013/V2I4201358.pdf
[5] Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Blackhole Attack In MANET
[6] X.P. Gao; W. Chen; A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks; IFIPInternational Conference on Network and Parallel Computing Workshops, 2007
[7] Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Wireless Broadband and Ultra Wideband Communications, Sydney, Australia
[8] Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communication.
[9] http://pushpita-pushpita.blogspot.in/2012/02/how-to-install-ns2-234-on-ubuntu-1004.html
[10] http://www.isi.edu/nsnam/ns/