Preventing MANET from black hole attacks within appropriate Area and Time

[1]Toofan Mukherjee, [2]Amit Kumar Bairwa, [3]Dr. Sandeep Joshi
[1]Research Scholar, [2]Assistant Professor, [3]Professor
[1]Computer Science and Engineering,
[1]Rajasthan Institute of Engineering and Technology, Jaipur, India

Abstract : A mobile ad-hoc network (MANET) is a collection of mobile hosts in which wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. Due to the characteristics of MANET like dynamic topology, the mobile ad hoc networks are vulnerable to different security threats. One of such security threat is black hole attack which is caused by the malicious nodes which takes part in the network activities. In Black hole attack, a malicious node drops all the traffic in the network to make use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and when the source node sends packet through it then it drops all the receiving packets. The performance of any protocol in presence of a malicious node heavily depends on the total area and the time of simulation.

***IndexTerms* - AODV, MANET, Security, Black hole, NS 2.**

I. INTRODUCTION

MANETs are often defined as follows: "A mobile ad-hoc network (MANET) is a collection of mobile hosts in which wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration" [1]. The MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily (lasting for a short time). In a MANET, nodes within each other's wireless transmission ranges can communicate directly; but yet, nodes outside each other's range have to rely on some other nodes to relay messages. Therefore a multi-hop scenario develops, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Each node functions as a router. So the success of communication highly depends on other nodes cooperation.

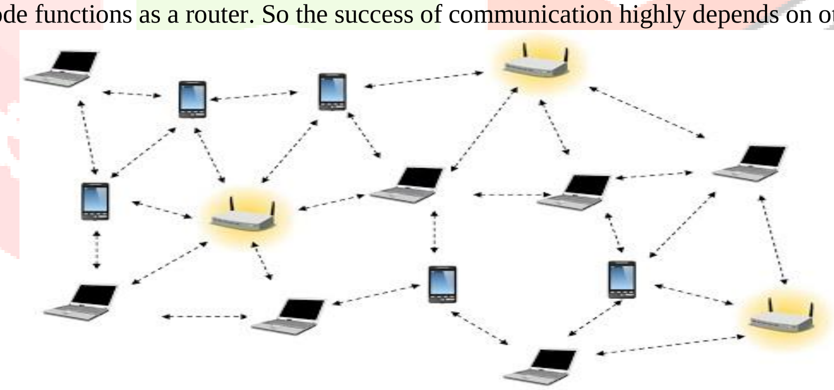

Fig 1.1 Wireless Ad-hoc network

However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes; one of these attacks is the Black Hole attack. In this attack a malicious node uses the routing protocol to advertise itself as having the shortest path to node whose packet it wants to intercept [2]. Black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. But the damage will be serious if malicious nodes work together as a group. Such type of attack is called cooperative black hole attack [3]. Actually the protocol to be analysed in our study is AODV (Ad-hoc on demand distance vector) protocol. In this paper we will be varying number of black hole nodes with respect to simulation area and simulation time on AODV routing protocol. But our focus is on Packet Delivery Fraction (PDF), End to End Delay (E2E Delay) and Normalized Routing Load (NRL).

II. LITERATURE REVIEW

2.1 SECURITY ISSUES FOR MANET

Vulnerability is a weakness in security structure. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. Subsequent are the various vulnerabilities that exist in wireless ad-hoc networks [4]:

i. **Open Medium** - Eavesdropping is easier than in wired network as there is no centralized medium.
ii. **Dynamically Changing Network Topology** – Mobile Nodes comes and goes from the set-up. They dynamically change their topology. So this will allows any malicious node to join the network without being detected [5].
iii. **Cooperative Algorithms** - The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security.
iv. **Lack of Centralized Monitoring** – MANET doesn't have a centralized monitor server or hub. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network. Deficiency of centralized management will impede trust management for nodes [6].
v. **Lack of Clear Line of Defense** - The only use of I line of defense attack prevention may not confident. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link.
vi. **Resource availability** -Resource availability is a major issue in MANET. If we provide secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and structural design. Collaborative ad hoc environments also allow implementation of self-organized security mechanism.

2.2 BLACK HOLE ATTACK

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.

III. ALGORITHM

Step1:blackholeaodv/blackholeaodv_logs.oblackholeaodv/blackholeaodv.o
Step2:blackholeaodv/blackholeaodv_rtable.oblackholeaodv/blackholeaodv_rqueue.o
Now, add following lines to ~/ns-allinone-2.35/ns-2.35/queue/priqueue.cc from line 93.
Step4: blackholeaodv patch
Step5: Case PT_blackholeAODV
To define new routing protocol packet type we have to modify ~/ns-allinone-2.35/ns-2.35/common/packet.h file. And we change PT_NTYPE to 74 and for our protocol PT_blackholeAODV = 73. From line 200 changes would be
Step6: // blackholeaodv packet
Step7: staticconstpacket_tPT_blackholeAODV = 73
Step8: // insert new packet types here
Step9: staticpacket_t PT_NTYPE = 74; // This must be the last one.
Then we make following code change at line 271 of ~/ns-allinone-2.35/ns-2.35/common/packet.h
Step10: type= = PT_AODV ||
Step11: type= = PT_blackholeAODV
And at line 351 of the same file, enhance the following
Step12: //blackholeAODV patch
Step13:Name_[PT_blackholeAODV]= "blackholeAODV";
Now we will modify tcl files to create routing mediator. Initially we define protocol name to use in tcl file. It would be done by modifying ~/ns-allinone-2.35/ns-2.35/tcl/lib/ns-packet.tcl at line 174.
blackholeaodv{
setragent [$self create-blackholeaodv-agent $node]
}
From line 864 of the same file following code should be added.
Step14: Simulator instproc create-blackholeaodv-agent {node} {
 # Createblackholeaodv routing agent
Set ragent [new Agent/blackholeaodv [$node node-addr]]
$self at 0.0 "$ragent start"

$node set ragent_$ragent
Return $ragent
}
Now we will set port numbers of routing agent. sport is source port and dport is destination port. Modify ~/ns-allinone-2.35/ns-2.35/tcl/lib/ns-agent.tcl from line 195
Step15: Agent/blackholeaodvinstprocinitargs {
$self next $args
}
Agent/blackholeaodv set sport_ 0
Agent/blackholeaodv set dport_ 0
At line 201 in ~/ns-allinone-2.35/ns-2.35/tcl/lib/ns-mobilenode.tcl, add the following
Step16: #Special processing for blackholeaodv
Set blackholeaodvonly [string first "blackholeAODV" [$agent info class]]
If {$blackholeaodvonly !=-1} {
$agent if-queue [$self setifq_(0)];# ifq between LL and MAC
}
Go to ~/ns-allinone-2.35/ns-2.35/ directory and do
Step17: make clean
Step18: make

IV. RESULT

4.1 PDF VARYING SIMULATION AREA AND BLACK HOLE NODES

The highest PDF is obtained at 500m when there was no black hole attack and lowest PDF is also obtained at 500m when the numbers of black hole nodes were three (3).

Table 4.1

PDF varying Simulation Area AND Black Hole nodes

Simulation Area (m^2)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole node=3
500	97.64	9.75	4.49	4.42
1000	94.04	20.09	13.3	10.8
1500	90.69	15.26	7.92	6.47
2000	41.53	14.92	12.92	10.31

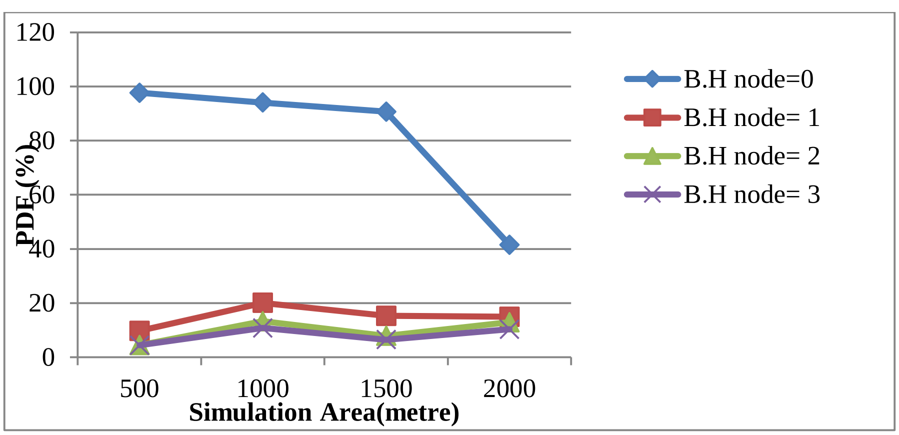

Fig. 4.1 PDF varying Simulation Area AND Black Hole nodes

4.2 PDF VARYING SIMULATION TIME

Refer to the above figure; we can see the effect of the black hole attack as the PDF decreases heavily as we increase the number of black hole nodes at all the simulation time. We can also observe that PDF is highest in normal conditions i.e. when there was no black hole attack and lowest when there were 3 black hole nodes present in the network. Highest & lowest PDF is observed at 1500 & 2000 seconds respectively.

Table 4.2

PDF varying Simulation Time AND Black Hole nodes

Simulation Time (Sec.)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole node=3
500	91.61	18.184	13.85	11.98
1000	93.1	17.35	9.61	9
1500	94.01	13.06	12.97	11.2
2000	91.91	12.43	11.04	8.57

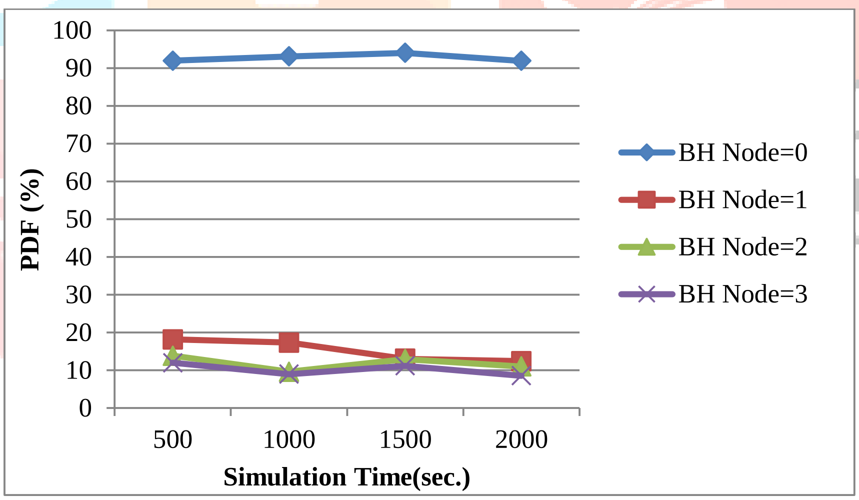

Fig. 4.2 PDF varying Simulation Time AND Black Hole nodes

4.3 AVERAGE END-TO-END DELAY

Refer to the above figure; we can clearly observe that the end to end delay increases rapidly as we increases the number of black hole nodes. The delay is highest at black hole node-2 and lowest is obtained at black hole node-0. There may be some fluctuation occurs in the result due to the position of black hole nodes at that time in the network.

Table 4.3

Average E-2-E Delay varying Simulation Area AND black hole Nodes

Simulation Area (m)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole node=3
500	15.06	12.7	15.22	16.41
1000	114.61	179.57	256.12	179.04
1500	225.69	615.19	260.65	210.36
2000	466.44	814.79	934.85	858.07

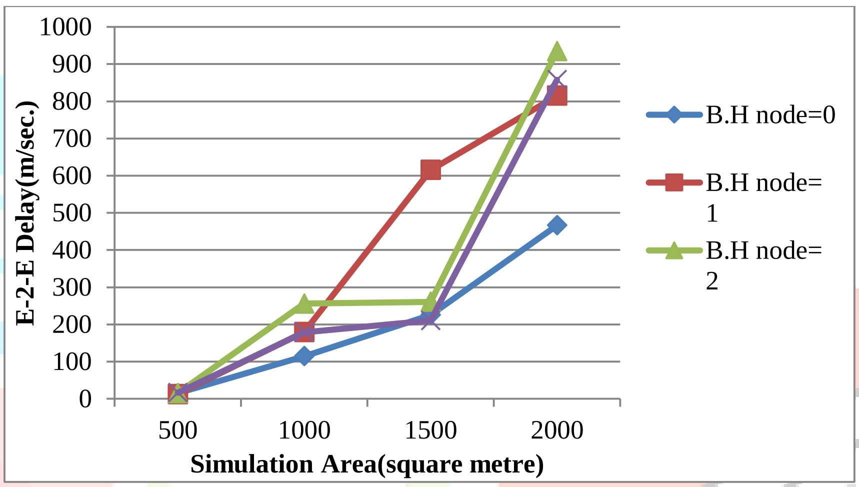

Fig. 4.3 Average E-2-E Delay varying Simulation Area AND black hole Nodes

4.4 END TO END DELAY VARYING SIMULATION TIME

Refer to the above figure; we can see that we have got the obvious result when the numbers of black hole nodes are varied with respect to the simulation area, end to end delay increase with respect to increase in black hole nodes.

Table 4.4

Average E-2-E Delay varying Simulation Time AND black hole Nodes

Simulation Time (Sec.)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole node=3
500	164.36	527.37	516.19	250.28
1000	133.57	213.79	284.96	474.76
1500	76.19	293.9	346.81	414.5
2000	135.55	204.23	301.53	8.57

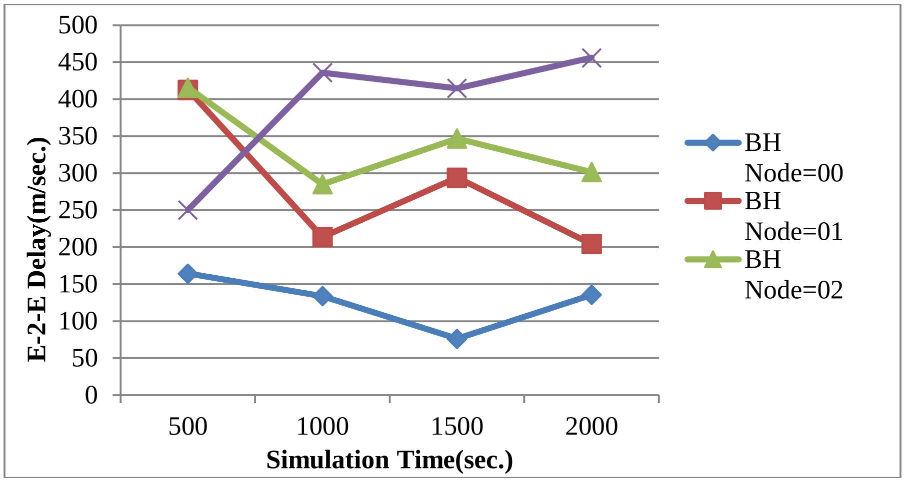

Fig. 4.4 Average E-2-E Delay varying Simulation Time AND black hole Nodes

4.5 Normalized Routing Load (NRL)

Refer to the above figure; it can be noticed that the routing load is highest when the number of black hole node is three but we can see that at some points (i.e. Black hole node-2).

Table 4.5

NRL varying Simulation Area AND black hole node

Simulation Area (m^2)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole
500	1.13	6.51	15.71	14.38
1000	2.88	13.35	14.8	14.94
1500	3.96	15.26	22.46	21.7
2000	3.36	10.3	10.1	12.52

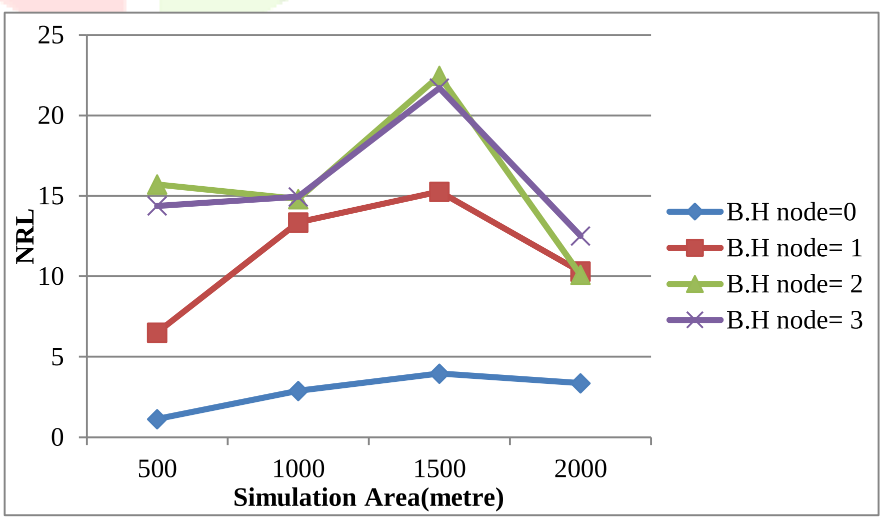

Fig. 4.5 NRL varying Simulation Area AND black hole node

4.6 NRL VARYING SIMULATION TIME

Refer to the above figure; we clearly see that the results are unexpected when the simulation time is varied with varying black hole nodes. Surprisingly the load is highest throughout all areas when one (1) black hole is present in the network. Although the NRL is least in case of no (0) black hole attack as expected.

V. Table 4.6

VI. NRL varying Simulation Time AND black hole node

Simulation Time (Sec.)	Black-hole node=0	Black-hole node=1	Black-hole node=2	Black-hole node=3
500	4.24	18.3	13.85	11.98
1000	3.3	15.48	9.61	9
1500	9.07	13.39	12.97	11.2
2000	2.83	19.01	11.04	8.58

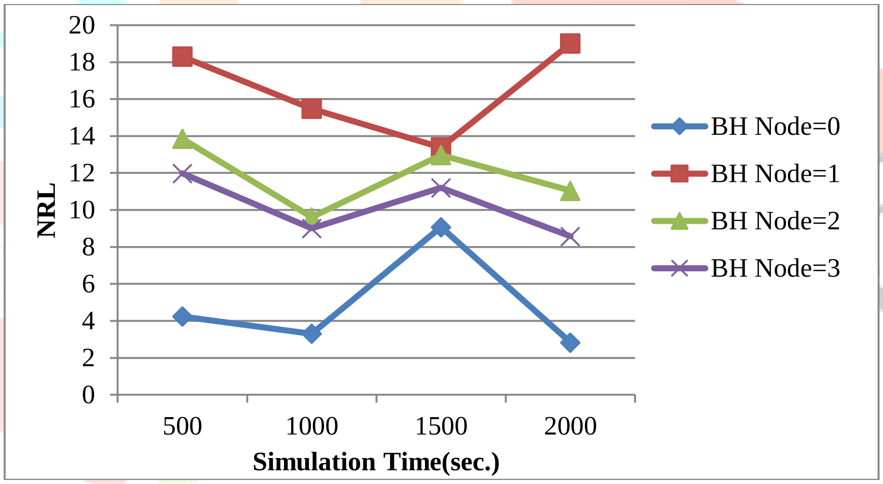

Fig. 5.6 NRL varying Simulation Time AND black hole node

V. CONCLUSION

The main objective of this paper is to compare the performance of the AODV routing protocol with varying the number of black hole nodes with respect to simulating area and simulating time in MANET. Through the results obtained from the simulation we can examine that Black hole has a huge effect on AODV protocol. Considering the case of PDF (Packet delivery fraction) varying both simulation are and time we can observe that the PDF is highest when black hole node was not present in both case. We get the obvious results that; we get the lowest PDF when there were Three (3) black hole nodes. Also we can note that we get the neck to neck results in all cases of black hole nodes.

After all the analysis we can conclude the performance of the AODV routing protocol heavily degrades in presence of a malicious node. Although since the observations are not real time and the results may vary in the realistic simulation environment, where the obstacles such as building will lead to the signal fading will also effects the performance of the network and protocol but still this research can be taken as an idea which selecting suitable simulation area and simulation time.

REFERENCES

[1] Ashis Bhattercharjee, Subrata Paul, "A Review on some aspects of Black Hole Attack in MANET", International Journal of Engineering Trends and Technology (IJETT) – Volume 10 Number 8 - Apr 2014.

[2] Puneet Kansal, NishantPrabhat, Amit, "Black hole attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 3, Issue 3, March 2013.

[3] Chanchal Aghi, ChanderDiwaker"Black hole attack in AODV routing protocol: A Review", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 3, Issue 3, April 2013.

[4] Elizabeth M. Royer, Santa Barbara, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks"International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[5] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, April 2013, in MECS (http://www.mecs-press.org/)

[6] Akanksha Saini, Harish Kumar ,"Effect Of Black Hole Attack On AODV Routing Protocol In MANET" IJCST Vol. 1, Issue 2, December 2010.

[7] Dr. Bvr Reddy, Monika Roopak, "Performance Analysis of Aodv Protocol under Black Hole Attack" , International Journal of Scientific & Engineering Research Volume 2, Issue 8, August-2011.

[8] Vishnu K, Amos J Paul, "Consequence of Cooperative Black/Gray hole attack in Mobile ad-hoc Networks", 2010 International Journal of Computer Applications, Volume 1 – No. 22.

[9] Robinpreet Kaur & Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs", International Journal of Computer Applications, Volume 45– No.22, May 2012.

[10] Swati Jain, Naveen Hemrajani "Detection and Mitigation Techniques of Black HoleAttack in MANET: An Overview", International Journal of Science and Research (IJSR), April-2011 India Online ISSN: 2319-7064.