IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Varying Black hole nodes in AODV routing protocol and evaluating its performance

[1]Mohammad Aamir Khan, [2]Kapil Kumawat
[1]PG. Scholar SBTC Jaipur
[2]Asst. Prof. SBTC Jaipur

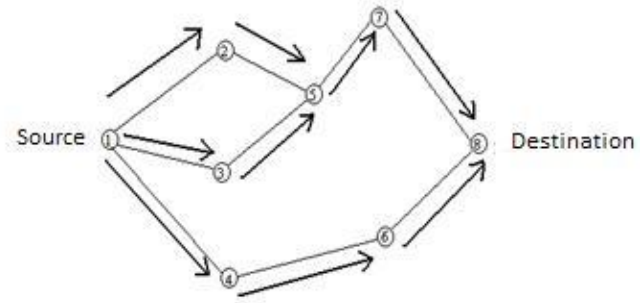
Abstract **- A Mobile ad-hoc network (MANET) is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Due to this it is vulnerable to various kinds of security threats. Black hole attack is one of such threats. This paper lead emphasis on AODV routing protocol in MANET, along with various types of security attacks and security threats with major concern on the Black Hole attack.**
Keywords - AODV, MANET, Security threats, Black Hole.

I. INTRODUCTION

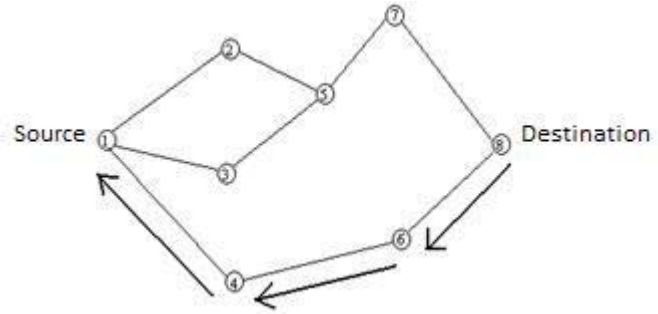
Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any layout. In this way, Ad-Hoc networks have a dynamic topology such that nodes can easily join or leave the network randomly. Thus this network is appropriate for areas where it is impossible to set up a fixed infrastructure [1]. In MANET, nodes offer connections by using different routing protocols including Ad-hoc on demand distance vector (AODV), Dynamic Source Routing (DSR), Destination Sequenced Distance Vector (DSDV) etc. The AODV is one of the widely used routing protocols in mobile Ad-hoc network. From the view of security aspect of the various routing protocols wireless Ad-hoc networks are not safeguard to malicious nodes attack among which Black Hole Attack is one of them in the network along with different types of attacks and which is described in later section of this paper.

II. AD-HOC ON DEMAND DISTANCE VECTOR (AODV)

The AODV routing protocol is a reactive routing protocol hence, paths are find when required. When a source node desires to send a message to some receiver node and it did not have a valid route to the receiver, the source node initiates a path finding process for allocating the other node. It broadcasts a route request (RREQ) packet to its nearby nodes, later transmitted further to their nearby nodes. This process continues to the extent up to which the receiver or an intermediate node with a "fresh enough" route to the destination is located. When the RREQ message packet either reaches the destination node or encounters a node with a route to the destination a response is entrusted. That response occurs via the transmission of a route reply (RREP) message. In case if a node realizes that the route is damaged or broken it transmits a route error (RERR) message to the source [2]. Figure 1 (a & b) below shows the working of AODV routing protocol.



(a) Propagation of Route Request(RREQ) packet



(b) Path taken by the Route Reply(RREP) packet

Figure 1.Working of AODV routing protocol

III. SECURITY ISSUES FOR MANETS

Ad-hoc networks are more vulnerable than wired networks therefore security is much more difficult to maintain. The various vulnerabilities that are associated in wireless ad-hoc networks are as follows:- [3]

Open Medium - Eavesdropping is easier than in wired network as there is no centralized medium.

Dynamically Changing Network Topology – Mobile nodes originates and terminate within the network and change their topologies rapidly which allows any malicious nodes to be added into the network without being detected.

Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security.

Lack of Centralized Monitoring – There is absence of any centralized infrastructure that prohibits any monitoring agent in the system.

Resource availability - Resource availability is a major issue of Mobile Ad-hoc Network. Security of information is done through various security schemas, layouts. Integrated Ad-hoc network also provides self organized security mechanism.

Scalability - Due to mobility of nodes, scale of ad hoc network changes randomly. So scalability is a major issue concerning protection of data in network. Security mechanism should be capable of handling a large network as well as small ones.

Limited power supply – Limited power supply is also a major obstacle for nodes of mobile Ad-hoc network and causes the node to behave in random manner.

IV. DIFFERENT TYPES OF ATTACKS IN MANET

Following are some types of security attacks possible in MANET :

Passive attack

Typically, passive attacks aim to steal the valuable information in at least two communicating nodes (as illustrated in Figure 2) or even in the whole network. There are many variations of passive attacks, but in MANET, there exist two types: eavesdropping and traffic analysis. Practically, depending on situations, passive attacks can be considered as legitimate or illegitimate actions. If the purpose is benign, for example, if the administrator wants to use some tools to probe the network traffic, in order to troubleshoot or account the network then it is legitimate. On the contrary, if the purpose is malicious, one attacker can steal valuable information by probing the network traffic such as credit card information, credential email, and then use the information to illegally withdraw money from bank accounts or blackmail the victims. Roughly speaking, passive attacks do not intend to disrupt the operation of the particular network.

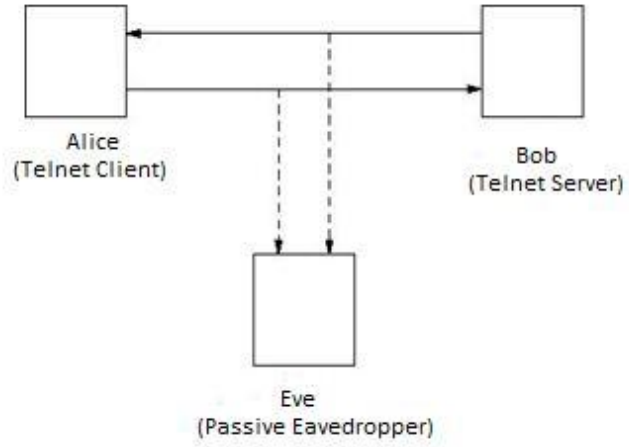


Figure 2. Passive attack

Different types of passive attacks are as follows:

- Traffic Monitoring
- Eavesdropping
- Traffic Analysis
- Syn flooding

Active attack

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost for the attacks. It causes editing of data stream or creation of false stream. Active attacks are able to alter the normal network operation. Typical example of active attacks can be: masquerade attack, replay attack, modification of message (illustrated in Figure 3) and Denial of Service (DoS). Active attacks can be internal or external.

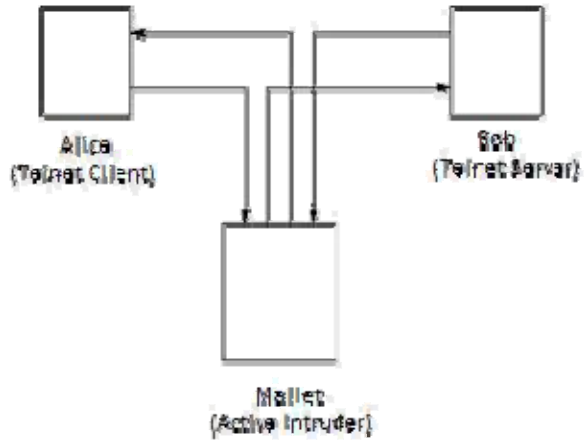


Figure 3. Active attack

External attacks are caused by nodes which are not the part of the network and internal attacks exist due to the nodes of the network which are more severe and complex in nature compared to the external nodes. If active attacks are done by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

Following are the various types of active attacks:

- Wormhole attack
- Black hole attack
- Rushing attack
- Location disclosure attack
- Flooding
- Sinkhole attack
- Spoofing attack
- Replay attack

V. BLACK HOLE ATTACK

A 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. The malicious nodes results in more damage to network if they work together in group which is termed as cooperative black hole attack. The initiation of Black hole Attack exists when malicious node looks out for other neighboring nodes to send RREQ information. When the information is received, the malicious nodes instantly sends a pseudo RREP information without confirming its routing table by including a sequence number of higher order to be in the routing table of the victim node before other node sends right information. Thus the requesting nodes gets illusion that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. [1]

Figure-3 shows the black hole attack. When a malicious node M enters the network it advertises that it has the shortest path to the destination node D when it receives the Route Request packets via node S. If node A responds earlier than the node M then it results in the failure of the black hole attack. The 1malicious nodes may dominate as it does not perform searching of the routing table for a route to the destination.

Also, the Route Reply packets originate directly from the malicious node and not from the receiver node. Thus , the malicious node is capable of replying faster than the node A as it does not perform searching like the node A, for a route to the destination node M, make free node M to listen all packets meant for destination node.

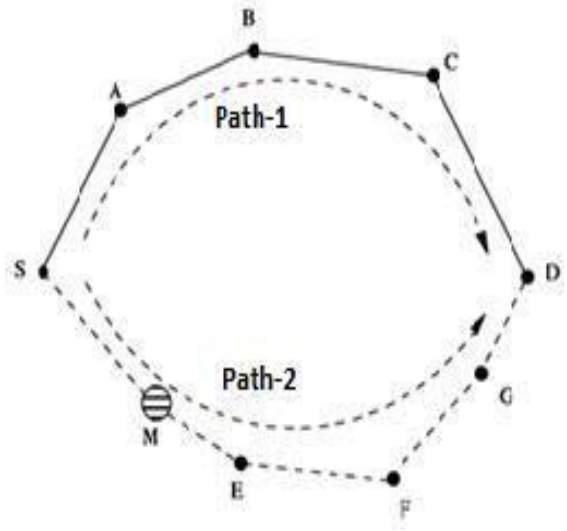


Figure 4. Illustration of Black Hole Attack

VI. SIMULATION ENVIRONMENT

A. Simulation Parameters

The simulation has been performed on Network Simulator version 2.35 (NS-2.35). We have simulated AODV routing protocol considering black hole attack. In our simulations, we have considered various number of black hole nodes. Also in our simulations, area and time have been varied.

Table 3-Simulation Parameters

Simulation Area	500 X 500, 1000X1000 1500x1500,2000x2000
Number of nodes	40
Number of black hole nodes	0, 1, 2, 3
Communication traffic	CBR
Maximum no. of connections	25
Simulation Duration	500, 1000, 1500, 2000 seconds
Pause time	2 seconds
Maximum speed of nodes	15
Radio Propagation model	Two ray ground
Packet rate	1 packet/sec
Number of Black hole nodes	1
Data Size	512 bytes

B. Simulation Metrics

Packet Delivery Fraction (PDF):- The packet delivery ratio in this simulation is defined as the ratio between the numbers of packets received by the CBR sink at destination to the number of packets sent by sources.

$$\text{Packet Delivery Fraction} = \frac{\text{CBR Packet received by CBR sinks}}{\text{CBR packets sent by CBR sources}}$$

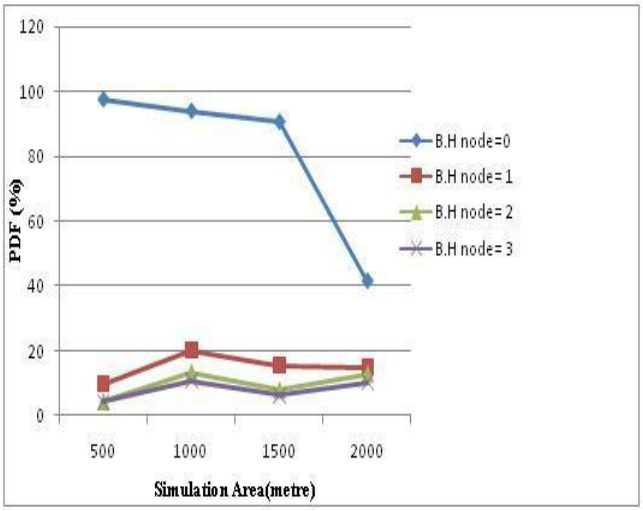
End-to-end delay :- The average time taken by the packets to pass through the network is called end-to-end delay. The time when a sender generates the packet and it is received by the application layer of pursuit, it is represented in seconds.

Normalized Routing Load :- NRL is the number of routing packets transmitted per data packet delivered at the pursuit. Each hop-wise transmission of a routing packet is counted as one transmission.

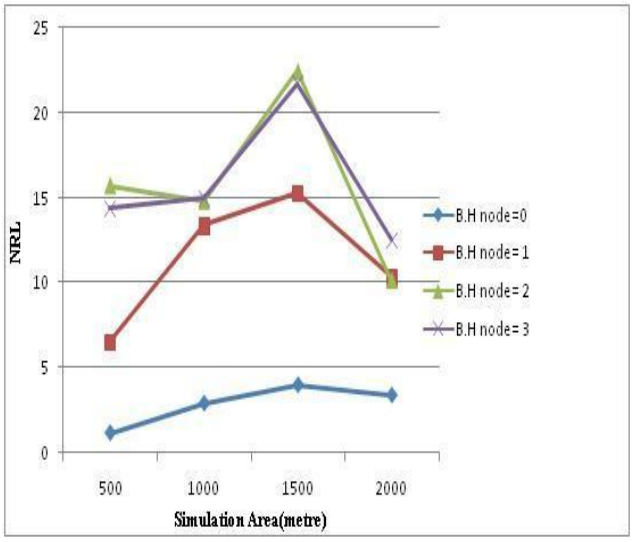
$$\text{NRL} = \frac{\text{Number of routing packets sent}}{\text{Number of routing packets received}}$$

VII. SIMULATION RESULTS

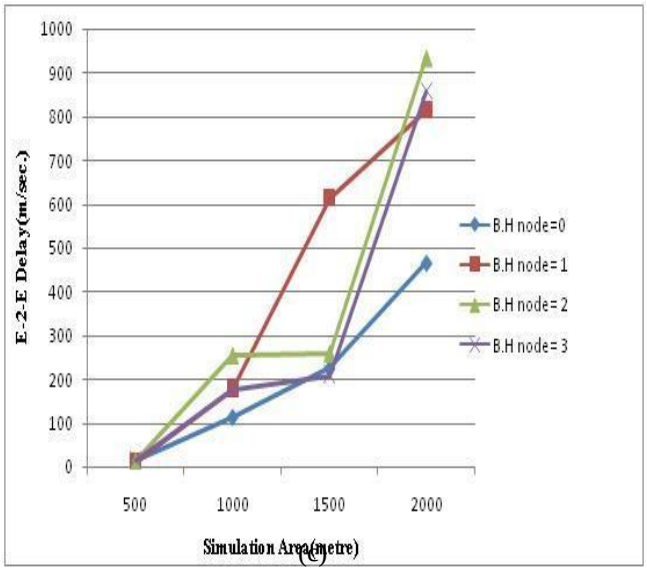
The analysis of simulation results is performed based on the standard metrics of Packet delivery fraction (PDF), Normalized Routing Load (NRL), End to End (E2E) delay. The simulation is carried out by varying simulation area and simulation time.



(a)



(b)



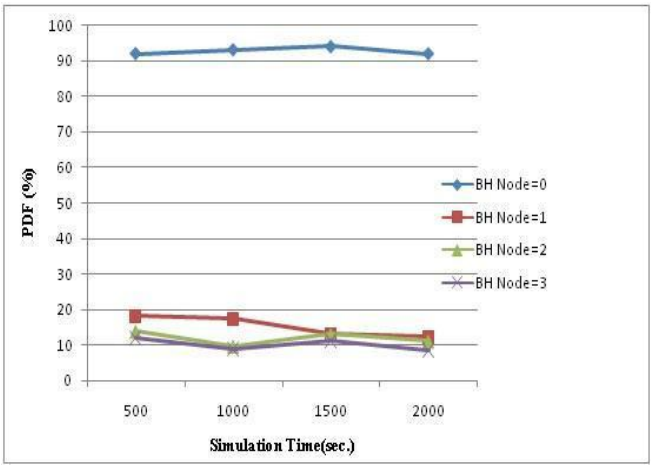
(c)

Figure 4. PDF, NRL and E-2-E delay varying number of black hole nodes with respect to simulation area.

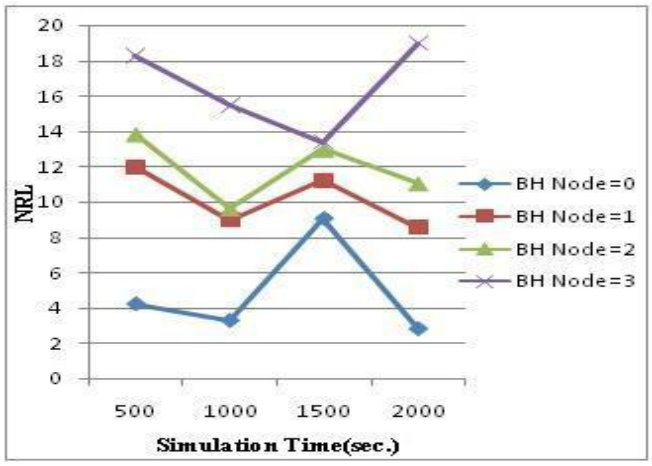
From the above figure, it can be observed that as the flashing of black hole nodes is increased onto the network, the PDF decreases and the NRL and the End to End delay increases. It can be found that when there is no black hole node present in the network PDF is high but as the presence of black hole nodes is marked and raised there is a gradual decrease in the PDF.

Now as far as NRL is concerned(figure b), it can be noticed that when number of black hole node is 2 and 3, the NRL goes neck to neck over the entire simulation area. But still the effect of black hole attack can be analyzed. The NRL is lowest when black hole node is not present at 500m and is highest when the black hole node is 3 at the simulation area of 1500m.

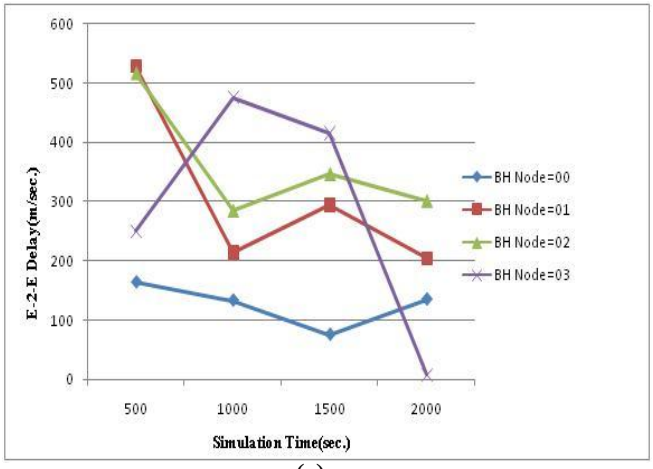
While observing the End to end delay, it can be observed that as the number of black hole nodes increases the delay also increases.



(a)



(b)



(c)

Figure 5 . PDF, NRL and E-2-E delay varying number of black hole nodes with respect to simulation time.

The above figure shows the effect of black hole attack by varying the simulation time. Figure (a) shows the PDF for the variation of the number of black hole nodes with respect to the simulation time. Here also it can observed that PDF is very high when there is no black hole node and is lowest when number of black hole nodes reaches to 3. However as the simulation time increases the values for PDF with various number of black hole nodes comes closer. Still it can seen that the effect is maximum when the number of black hole nodes is 3.

Now considering the effect of black hole attack on the NRL and the end to end delay, it can be seen that when the number of black hole nodes in the network is increased, the effect becomes more brutal. However it can be noticed that the delay when number of black hole nodes is 3 at simulation area of 2000m is very much unexpected. But still it can be analyzed that the end to end delay and the normalized routing load increases with the increase in the number of black hole nodes.

VII. CONCLUSION

In this paper, the various aspects of security issues and attacks possible in MANET. In this paper the focus have been led onto analyzing the effect of black hole attack considering various number of black hole nodes. As expected it is observable that with the increase in the number of black hole nodes, the performance of the network degrades and also the effect of black hole attack is more severe with the variation in simulation time. It can also be noticed that the packet delivery fraction is inversely proportional to the NRL and the end to end delay. So, by the results shown in this paper considering different number of black hole nodes varying both simulation

time and simulation area, it can be concluded that the black hole attack can have a very severe effect on the network.

REFERENCES

[1] A. Vani ECE Department CBIT-Hyderabad D. Sreenivasa Rao Professor ECE. Department, JNTU Hyderabad, Andhra Pradesh, India "Removal of Black Hole Attack in Ad Hoc Wireless Networks to provide confidentiality security service".

[2] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90–100.

[3] Akanksha Saini, Harish Kumar Department of Computer Science & Engineering, UIET, Punjab University Chandigarh, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET".

[4] Ingo Gruber, Oliver Knauf and Hui Li," Performance of Ad Hoc Routing Protocols in Urban Environments", In Proceedings of European Wireless 2004 (EW'2004, Barcelona, Spain, February 24 - 27, 2004, Barcelona, Spain

[5]http://www.cubinlab.ee.unimelb.edu.au/~jrid/Docs/ Manuel-NS2/node196.html.

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

[7] Dr Karim KONATE and Abdourahime GAYE, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking Vol. 4, No. 2, June, 2011.

[8] Abhinav Mehta, Rohit Jain, Vinay Somani "Comparison of various Radio Propagation models on AODV with and without Black Hole attack in MANET", International Journal of Computer Applications (0975–8887), Published by Foundation of Computer Science, New York, USA. Vol. 61, No. 2, January 2013.

[9] Sheenu Sharma, Dr. Roopam Gupta, "Simulation Study of Black hole Attack in the Mobile Ad hoc Networks", 21-22 November 2008.

[10] "Simulation of Black Hole Attack In Wireless Ad-Hoc Networks", A Master's Thesis In Computer Engineering Atlim University by Semh dokurer September 2006.

[11] 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.

[12] Dr.Ibrahim khider, Prof. Wang Furong, Amna Saad, "The effect of two realistic Radio Propagation Models for Mobile Ad hoc Networks in Urban Area Environment Supported with stations", International Journal of Scientific & Engineering Research Volume 2, Issue 10, Oct-2011.