ENSC 427 Communication Networks

Black-hole Attack in Mobile Ad-Hoc Network

Final Project

Spring 2015

Final Report

Group 4

SeungJun Lee (John) sjl14@sfu.ca

Paul Chen pfc3@sfu.ca

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronyms Extended Form

ADOV – Ad-hoc On-Demand Distance Vector

NAM – Network Animator

NS-2 – Network Simulator 2

RREQ – Routing Request

RREP – Routing Reply

MANET – Mobile Ad-hoc Network

IP – Internet Protocol

Abstract

Mobile devices cannot be separated from our daily life, and they can construct network proactively to exchange information where the conventional communication infrastructure are not exist. We call this kind of network environment as Ad Hoc Network. However, the Ad Hoc Network has vulnerability in data security due to its characteristics of network protocol. The Black Hole Attack is the major risks in the Ad Hoc Network as an attacker makes faulty route by responding fake network information to the information source**,** and intercepts data through faulty route they made. In this project, an Ad Hoc Network is to be constructed, and analyze the results from the simulation of the Black Hole Attack by using the NS-2.

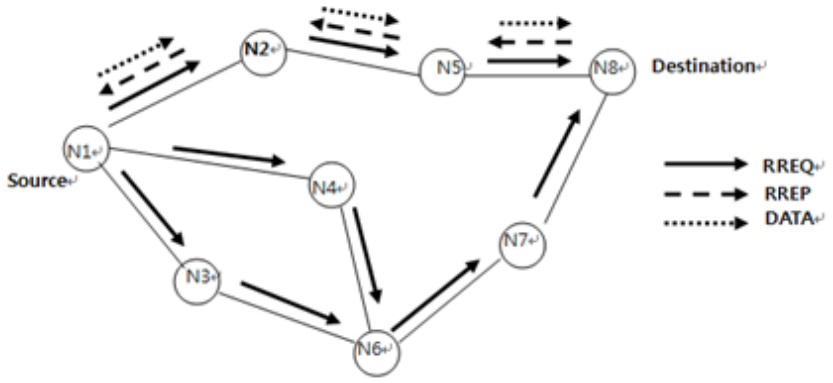
1. Introduction

With technology development and the widespread of mobile devices, people need new network environment fulfilling their various needs in different areas, and performing tasks by connecting internet and networks without limiting time and places. The wireless networks meet the needs. Wireless networks can be classified in two areas; infrastructured network using facilities such as base station and access point, and infrastructureless network composed with mobile devices. We call this infrastructurless network as Ad hoc network. Each mobile terminal device has a node, and the nodes need routes to exchange data packets between the nodes. There are two routing protocol in Ad hoc networking; Table-driven and On-demand. The DSDV(Destination Sequenced Distance Vector) protocol is the typical routing protocol in the Table-driven (proactive) protocol, which has latency and overheading problem in network. The protocols in On-demand routing are DSR(Dynamic Source Routing) and AODV(Ad hoc On-Demand Distance Vector) protocol. AODV is more efficient routing protocol compare to other protocols, because AODV keeping only new updated routing data, and suitable for Ad hoc network. In AODV, a node broadcast a request (RREQ) to neighbor nodes to find route to send packets, and the receiving node sends Route Response (RREP) to the neighbor. There are many intermediate nodes between the source and destination node, so nodes between them send RREP with route data in the reverse direction. The source node starts routing the packets to the destination node via the neighboring node which responded with RREP. The most important aspect is to analyze the Black-hole attack in Ad-hoc On-Demand distance Vector (AODV) Routing. The Ad hoc network with AODV protocol has condition to the so-called Black Hole attack. A black hole is a node which always respond fake positive routing reply (RREP) message to the every routing request (RREQ), and create new false route. Once the data packets form source node reach black hole node, the packets will be intercepted. This report will describe an overview of Black-hole attack in Ad-hoc On-Demand distance Vector Routing network models. The NS-2 code implementation will be described the black-hole attack in ADOV routing network system.

2. Backgrounds

2.1 Ad-Hoc On-Demand Distance Vector (AODV)

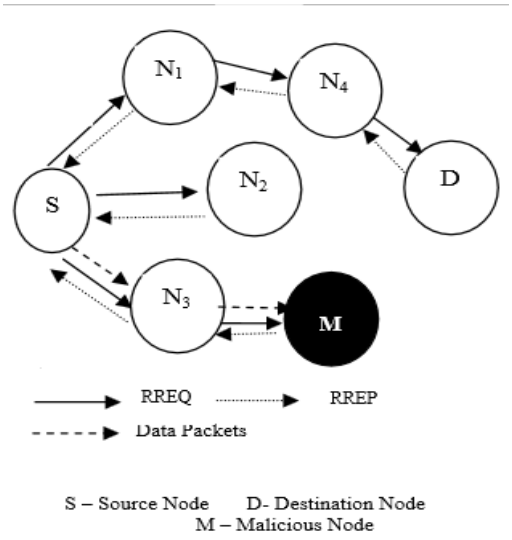
There are two steps of operation in AODV; Route Discovery and Route Keeping by using the destination sequence number. When a route is needed for data transfer, a route discovery process is to be initiated by broadcasting PREQ message to the neighbor nodes. On the paths of transferring PREQ to the destination node, if any of intermediate nodes received the PREQ have route information for the destination, the intermediate node sends PREP message in the unicast method back to the source node which generated the PREQ. On the other hand, the intermediate nodes which do not have the route information for destination broadcast PREQ to their neighbor nodes. PREP message is unicasted back to the node previously received PREQ. If any links are failed or errored due to the displacement or extinction of nodes, a recovery process will be started, or PERR message is to be transferred to the source node to delete the routing information of the failed link, and initiate resume a route discovery process



[Figure 1] - RREQ and RREP process in AODV [6]

2.2 Black-Hole Attack

With the nature of algorithm of Ad Hoc On-Demand Distance Vector (AODV) protocol, Black Hole Attack has been a major concern of network security in AODV. If packets need to be transferred to the destination node, the PREQ route request message is to be broadcasted to the neighbor nodes, then intermediate nodes which received PREQ send their neighbor over and over until the route reaches destination, and send PREP with route information back to the source node. The source has entries of route information, and sends data to destination using fresh route. With the purpose of packet interception, malicious nodes which act as destination node by responding positive PREP at all times can be designated in the middle of paths between source and destination. Once packets reach the malicious nodes, the packets will be intercepted.



[Figure 2] - Blackhole attack Process [7]

3. Network Simulation

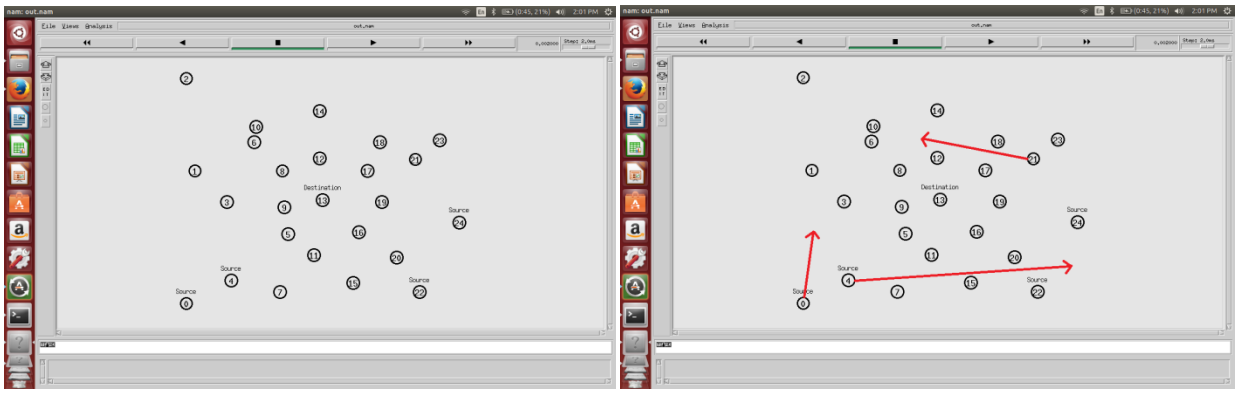
Scenario 1: MANET without blackholes

Total 25 nodes are used in this model, including four Source Nodes (N0, N4, N22 and N24) and one Destination Node (N13). The route discovery and data transfer process between source node-0 and 4, and destination node N13 were done successfully through intermediate nodes N6, 7, 9 and 17 respectively including one direct transfer between source node N4 and destination node N13. With the mobility function applied to the nodes, this simulation tried to cover real mobile communication environment. In the very beginning of simulation, the source node starts moving upward in the screen, then N0 starts transmitting packet data to the destination N13, then our simulation goes on using different source and routes with mobility function applied. 12 times of packet transfers through 12 different routes and nodes were succeeded during our simulation time.

The table1 shows the routes used for data transfer are;

Source	Intermediate	destination	Source	Intermediate	destination
N0 ====> N7 ====> N13			N0 ====> N6 ====> N2		
N4 ====> N9 ====> N13			N4==========>N13		
N4 ====> N7 ====> N13			N4====>N19===>N21		
N4 ====> N16 ====> N21			N4====>N20===>N21		
N22 ====> N16 ====> N21			N24==========>N21		
N24 ====> N23 ====> N21			N24=>N23=>N19=>N21		

[Table 1] – Packet transfer through different routes and nodes in scenario1



[Figure 3] - Nam display for 25 nodes in scenario1 model.

We also analyze Jitter and Throughput of Node 2 and Node 21 using trace analyzer. Understanding that the Jitter is packet transmission delay, and determined by different factors such as processing time, queuing, transmission and propagation delay. The packet transmission delay can be described as:

Packet Delay(Jitter) = d(proc) + d(queue) + d(trans) + d(prop) (equation 1)

d(proc) : header processing delay of router

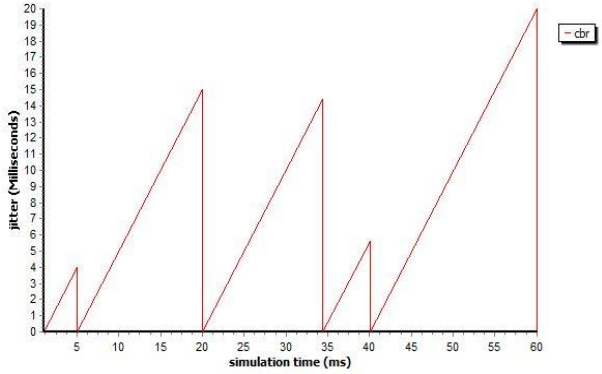
d(queue): time for query of a packet

d(trans): delays depend on network speed

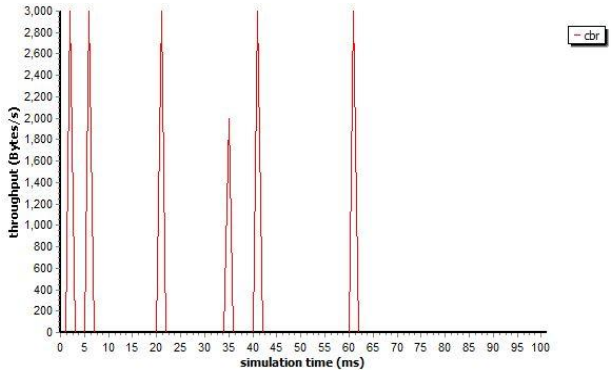
d(prop): propagation delays depend on physical medium of network connection and distance [10]

The [Figure 5] shows that there were 6 events of packet transfer at different time frames of 1, 5.9, 20, 25, 32 and 33.5sec respectively with the 5 different paths, and Figure:4 shows that there had been packet delays(Jitter) for each packet transfer. Packet delivery through the route N0-N7-N13 took little delay, and the route N4-N7-N13 took long delay. The delay mostly depends on network speed, header processing of router and query of packet for transfer.

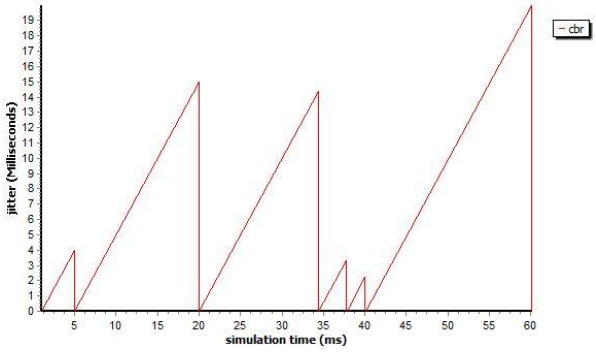
The [Figure 8] shows that there had been no packet losses during the transfers in Scenario-1 simulation.



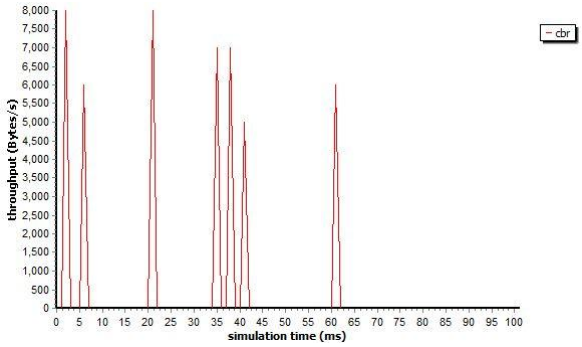
[Figure 4] - Jitter of the node 2 in our scenario1



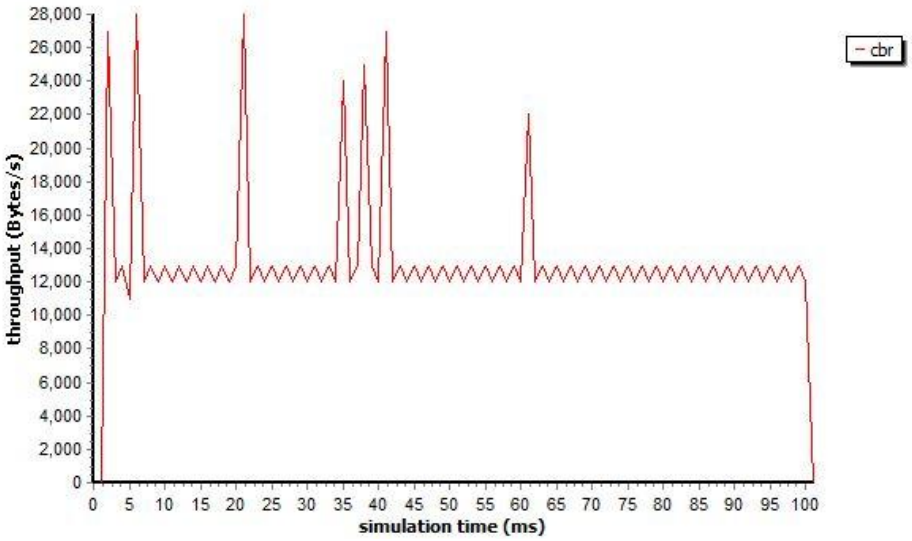
[Figure 5] - Throughput of the node 2 in our scenario1



[Figure 6] - Jitter of the node 21 in our scenario1



[Figure 7] - Throughput of the node 21 in our scenario1



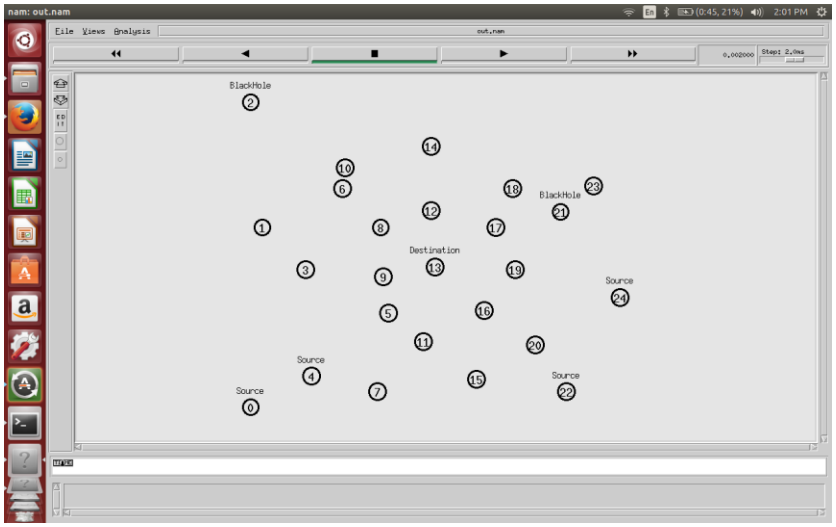
[Figure 8] - Throughput of the destination node 13 in our scenario1

Scenario 2: MANET with Blackholes

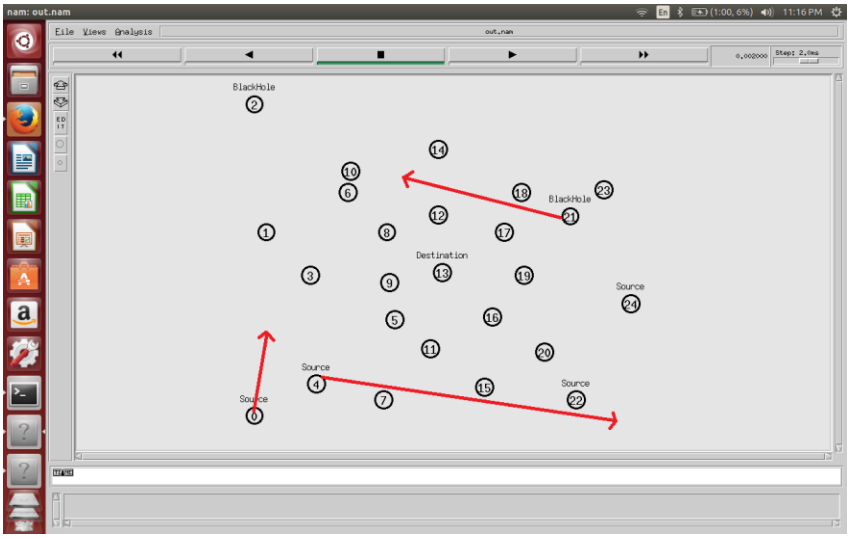
By putting nodes N2 and N21 into the network, which act as 'Black Hole' maliciously intercepting data from the route between the source and destination by responding deceptive RREP message to the source node, this scenario model simulates Black Hole attack situation. The simulation performed via different routes of node 0-6-2, 4-19-21, 4-16-21, 4-20-21, 22-20-21, 22-20-19-21, 22-20-21, 24-21, 24-23-21 and 24-23-19-21 respectively. As shown in [Figure 15], the data throughput between the source and destination was significantly decreased due to packet drop to the Black Hole during 40-100sec. On the other hand, as shown in [Figure 14], the data throughput to the Black Hole was significantly increased for black hole nodes 2 and 21 during the time duration of 5-25sec and 30-100sec when the black holes were activated.
The table2 shows the routes used for data transfer are;

Source	Intermediate	destination	Source	Intermediate	destination
N0 ====> N7 ====> N13			N0 ====> N6 ====> N2		
N4 ====> N9 ====> N13			N4==========>N13		
N4 ====> N7 ====> N13			N4====>N19===>N21		
N4 ====> N16 ====> N21			N4====>N20===>N21		
N22 ====> N16 ====> N21			N24==========>N21		
N24 ====> N23 ====> N21			N24=>N23=>N19=>N21		

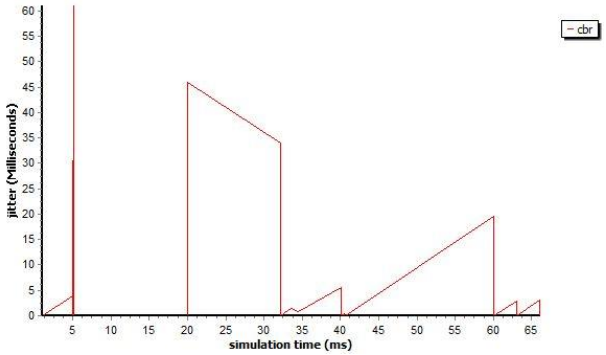
[Table 2] – Packet transfer through different routes and nodes in scenario2



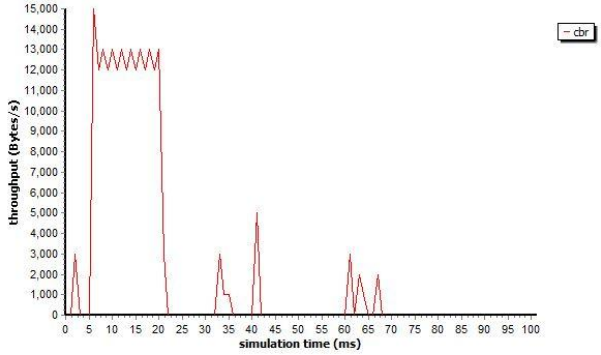
[Figure 9] - Nam display for 25 nodes in black-hole attack model.



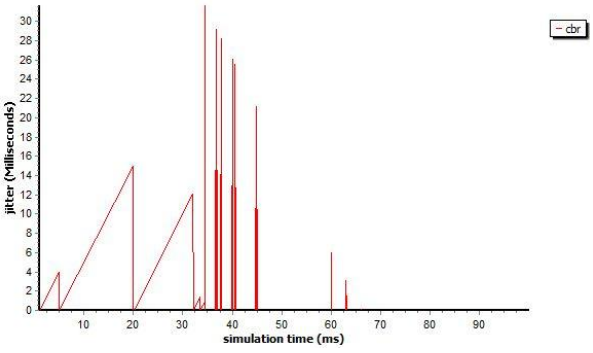
[Figure 10] - Nam display for node 21 shifts to support the black-hole attack node model



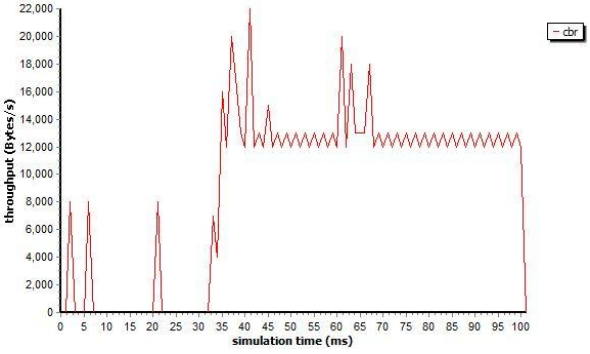
[Figure 11] - Jitter of the node 2 in our scenario2



[Figure 12]- Throughput of the node 2 in our scenario2



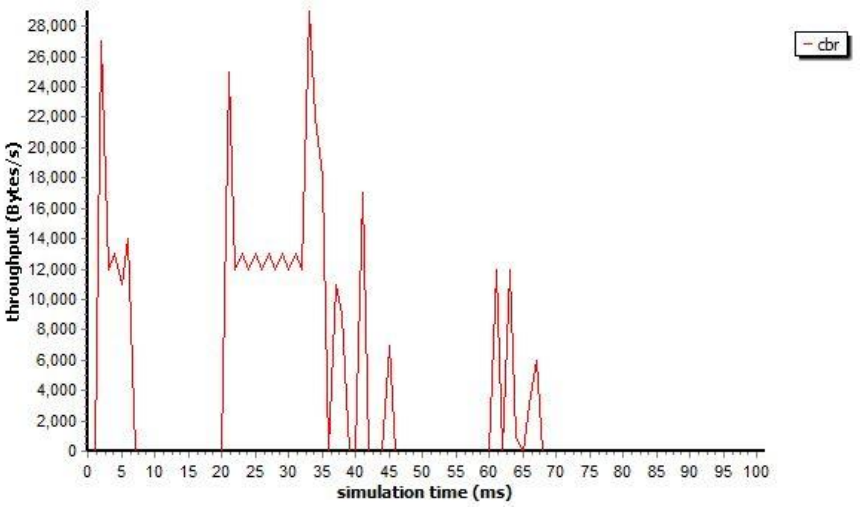
[Figure 13] - Jitter of the node 21 in our scenario2



[Figure 14] - Throughput of the node 21 in our scenario2

We also analyze Jitter and Throughput of Node 2 and Node 21 in scenario2 using NS-2 trace analyzer. Understanding that the Jitter is packet transmission delay, we see there are delays on each packet transfer. Because digital communication circuits needs delay buffer, and the size of

buffer need to be determined, the jitter must be measured and applied to the device. The figures shown in right hand side show data amounts transmitted through different routes.



[Figure 15] - Throughput of the destination node in our scenario2

You can see the significant differences in packet delay (Jitter) for the Black Hole node N2 and N21. The delay factors depend on network traffic, speed and medium of physical link between source and destination.

4. Future Work

Study for understanding wireless network security for attacks such as Warm hole, Gray hole and Black hole will be done in the near future, and also my special studies for preventing black hole attack will be done. Developing skills to use NS-2 is also important for me to deal with networks.

5. Conclusion

Mobile ad-hoc networks are useful in the place where fixed communication infrastructure is not available, and able to construct network in a proactive manner using mobile devices. But it also has significant vulnerability to the security threats such as ‘Black Hole’ attack which maliciously reside in the mobile ad hoc network to intercept data. With its nature broadcasting request and acknowledgement to the neighbor nodes, malicious nodes can be put into network, which always generate fake positive acknowledgement signal to the source to intercept packets, we call it ‘Black Hole Attack’. Our simulation showed how Black Hole Attack worked on the Mobile Ad Hoc Network.

6. Reference

[1] A. Leon-Garcia and I. Widjaja, Communication *Networks: Fundamental Concepts and Key Architectures*, 2nd Ed. New York: McGraw-Hill, 2004.

[2] C.E. Perkins, E.M. Royer, *Ad-hoc on-demand distance vector routing*, Mobile Computing Systems and Applications, 1999. Proceedings, WMCSA '99. Second IEEE Workshop on, pp. 90-100, 25-26 Feb 1999.

[3] E.A Mary Anita, and V. Vasudevan, *Black hole attack prevention in multicast routing protocols for mobile ad hoc networks using certificate chaining*, International Journal of Computer Applications, 2010, Vol, no, 1-12, pp 21-28.

[4] E. H. Teerawat Issariyakul. *Introduction to Network Simulator NS2*. Springer US, Springer.com, 2009.

[5] G. I. Papadimitriou, A. S. Pomportsis, P. Nicopolitidis, and M. S. Obaidat *Wireless Networks* pg 291-292, John Wiley and Sons Ltd, December 2002

[6] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, pp 70- 75

[7] K. Lakshmi, S.Manju Priya, A. Jeevarathinam K.Rama, K.Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", In- ternational Journal of Engineering and Technology.

[8] M. Al-Shurman, S. Yoo, and S. Park, *BlackHole Attack in Mobile Ad hoc Networks, ACM Southeast Regional Conference*, pp. 96-97, 2004(ACM-Se' 42), Huntville, Alabama, 2-3 April 2004.

[9] M. Greis, *Marc Greis Tutorial for the Network Simulator NS-2*.

[10] R. S. Chawla, (2013, Sept 3). Computer Networks: Delay in Transmission. [Online]. Available: http://com2networks.blogspot.ca/2013/09/delays-in-transmission.html

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J.Dixon, and K. Nygard, *Prevention of Cooperative BlackHole Attack in Wireless Ad hoc Networks.* Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.