International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 2, March - April 2017 ISSN 2278-6856

ANALYSIS OF BLACK HOLE ATTACK ON AD HOC NETWORKS USING VARIOUS MOBILE AD HOC NETWORK ROUTING PROTOCOLS

Dr. CHANDRA NAIK M[1], Dr.G.SAMBASIVA RAO[2]

[1,2]Professor, Nawab Shah Alam Khan College of Engineering &Technology,
New Malakpet, Hyderabad, Telangana State, India-500024

Abstract: ***In this scenario, ad hoc networks are gaining quality to its peak today, as the users want, an ad hoc connectivity irrespective of their GIS position. If there is more than threat of attacks on the MANETs. Black hole attack is one of the privacy threat in which the traffic is redirected to such a node that actually does not exist in the network. It is an analogy to the black hole in the universe in which things to discontinue to be seen. The host to host presents it 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 privacy way for transmission and communication which is quite challenging and characteristic issue. In order to provide privacy communication and transmission, researcher worked specifically on the privacy issues in ad hoc networks, and many privacy routing protocols and privacy measures within the networks were discussed. Presently the works done on privacy issues in ad hoc network were based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were detailed by stating how these attacks disrupt the performance of MANET. The perceptions of this thesis is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc On Demand Distance Vector (AODV).The collision of Black Hole attack on the completeness of ad hoc network is evaluated finding out which protocol is more effectible to physical to the attack and how much is the collision of the attack on both protocols. The collection of data was taken in the light of output, end-to-end desired and network load. Network simulation is done in Optimized Network Engineering Tool (OPNET).***

Keywords: MANET, Black Hole, Routing Protocol (RP)s and NS-2 Simulator**.**

1. INTRODUCTION

Mobile Ad-Hoc Networks is an independent and decentralized wireless network system. Mobile ad hoc networks consist of ad hoc mobile nodes that are free in moving in and out in the network. Nodes or devices i.e. mobile phone, laptop, personal computer digital assistance, MP3 player and PC that are participating in the network and are mobile. In this nodes act as host/router or both same at the time. They can form impulse topologies depending on their connectivity with one to another in the network. These nodes have the acquired to configure itself and because of their self configuration state of able, without the need of any an underlying base. Internet Engineering Task Force has ad hoc network working group (WG) that is devoted for developing IP routing protocols. Routing protocol (RP) is one of the challenging and interpretation of facts. Many (RP) have been is workable for mobile ad hoc networks, i.e. AODV, OLSR, DSR, ODMRP, AM Route etc. Privacy in MANET is the concern for the basic program of network. The capability of communications, intimacy and integrity of the data can be performed by assuring that privacy issues have been met. An ad hoc network often suffer from privacy attacks because of its features like open medium, absent of central cautions and manages, cooperative algorithms and no instance mechanism.

1.1 Problem Statement

Previously the works done on privacy issues i.e. attack (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV).

1.2 Motivation

Privacy in MANET is the concern for the basic the kind of action of network. Capable of network services, communicated in confidence and integrity of the data can be achieved by assuring that privacy issues have been met. MANET often suffer from privacy attacks because of its features like open medium, lack of central actions and management, cooperative algorithms and no instance mechanism.

1.3 Work Related

MANET is very much popular due to the fact that these networks are dynamic, an underlying baseless and scalable. Links also makes the MANET more effect to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Several types of attacks have been analyzed in MANET and their affect on the network. Attack such as gray black hole, where the attacker node behaves spitefully for the time until the packets are dropped and then switch to their normal behavior [11]. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker by neither using RREQ nor data flooding [12].

2. WIRELESS NETWORKS

Wireless networks are gaining quality to its point today, as the user wants wireless communication irrespective of their GIS position. Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the main reasons of the quality of these networks is widely organization of wireless devices. Connectionless application and devices mainly stress on Wireless Local Area Networks. This has mainly two modes of processes, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. Ad-Hoc networks do not depend on fixed an underlying base in order to carry out their processes.

2.1 Network

Before going into the details of wireless network, it is significant to understand what a network is and several types of networks available now days. Any collection of devices/computers connected with each other by means of communication channels that help the users to share resources and communicate with other users. There are two categories of network i.e. wired and wireless networks.

2.2 Why Wireless Networks?

Wireless networks are getting popular due to their easy of useful. Consumer/user is no more dependent on wires where he/she is, ease to move and enjoy being communicated to the network. One of the great features of wireless that makes it fascinating and different amongst the traditional wired networks is quality. On the basis of coverage area the wireless communications can be divided into three types.

a) Personal Area network
b) Local Area Network
c) Wide Area Network

a) Personal Area Network

PANs are used for communication between computers devices close to one person [1].Some of the PANs are zigbee, Bluetooth, sensor networks. Bluetooth is low/high cost wireless connection that can link up devices. These devices work within 100 meters, with access speed up to 1221 Kbps.

b) Local Area Network

Wireless local area network is standardized by Institute of Electrical and Electronics Engineer (IEEE). In LAN the users communicate with each other in local area coverage i.e. within building or campus. It implemented in mobile devices like a laptop, PDAs, Mobile Cell phones etc. In Wired LAN, Ethernet Protocol, IEEE 802.11 is used. Wired LAN is mainly used for the connection with internet.

c) Wide Area Network

Wireless wide area network (WWAN) cover GIS larger area than LAN. The WANs almost consist of one or two LANs.

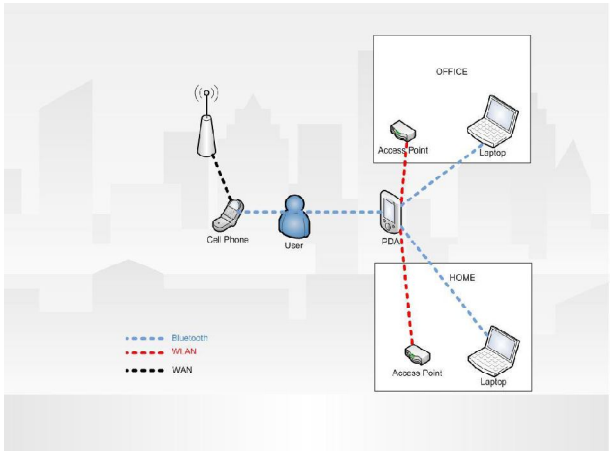

Fig. 2.1 Communications in Wireless Networks

2.3 Route Discovery Mechanism in AODV

Node "A" wants to initiate transmission with another node "G" as shown in the Fig. 2.2 it will generate a route request message (RREQ). Once the host node is located or an intermediate node with enough fresh routes is in particular location, they generate control message route reply message (RREP) to the host node. When RREP reaches the host node, a route is established between the host nodes "A" and host node "G". Once the route is established between "A" and "G", node "A" and "G" can network with each other.

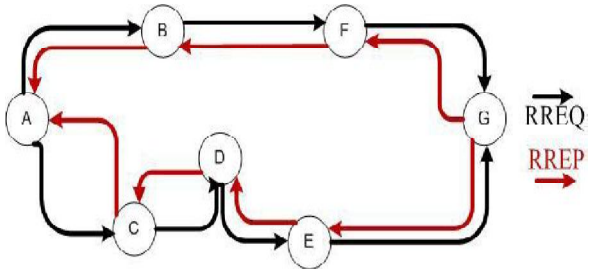

Fig. 2.2 AODV Route Discovery

When there is a link up/down or a link between hosts is broken that causes one or more than one links not reachable from the host, the RERR message is sent to the host. When RREQ message is broadcasted for the positioning the host i.e. from the node "A" to the next to another nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the host informing the host a route error, where "A" is host and "G" is the host. As shown in the Fig.2.3

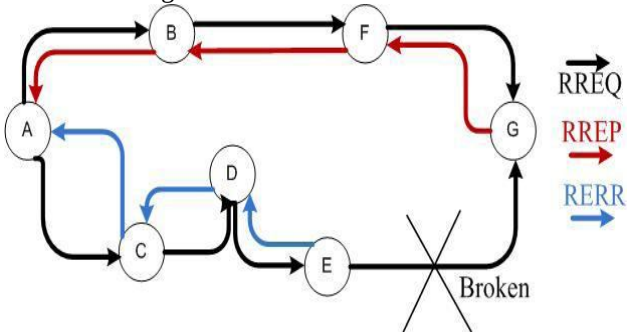

Fig. 2.3 Route Error Message in AODV

3. PRIVACY ISSUES IN MANET

Privacy in MANETs the concern for the basic the quality of network. Capability of communications, intimacy and integrity of the data can be performed by assuring that privacy issues. MANET often suffers from privacy attacks because of its features like open medium, several topologies dynamically, lack of central monitoring and manages cooperative algorithms and no instance mechanism. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of privacy [15]. The RPs designed majorly for internet is different from the MANET. Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone [16].

3.1Classification of Attacks

The attacks can be categorized on the basis of the host of the attacks i.e. Internal /External, and on the behavior of the attack i.e. Passive/Active attack. This classification is most uses because the attacker can an act the network either as internal, external or/ as well as active/passive attack.

3.1.1 External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, DoS in order to disrupt the performance of the whole network. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network.

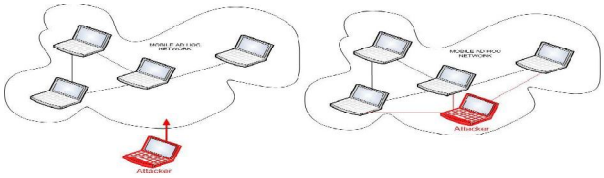

Fig. 3.1 External and Internal Attacks in MANETs

3.1.2 Active and Passive Attack

In active attack the attacker interrupts the performance of the network, uses information and tries to destroy the data during the exchange in the network [10]. This attack brings the attacker in powerful position where attacker can't modify, fabricate and replays the massages. Attackers in passive attacks can't interrupt the processes of the network [10].

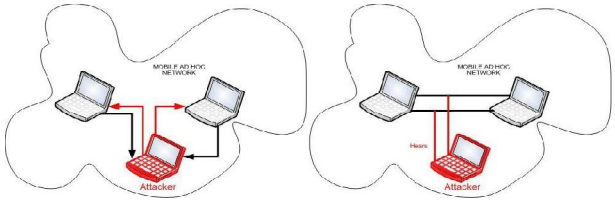

Fig. 3.2 Active and Passive Attack in MANETs

4. BLACK HOLE ATTACK IN MANET

MANETs face different privacies threats i.e. attack that are carried out against them to disorder the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET).

4.1 Black Hole Attack

In this scenario, Black hole attack, a spiteful node uses its RP in order to purpose itself for having the shortest path to the host or to the packet it wants to deflect. In this way attacker node will always have the availability in replying to the route request and thus deflect the data packet and retain it [15]. As shown in Fig. 4.1 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 spiteful node then it will claim that it has active route to the specified host as soon as it receives RREQ packets.

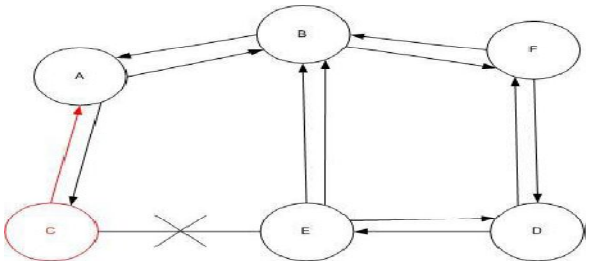

Fig. 4.1 Black Hole Problem

4.1.1 Black hole attack in AODV

There are two categories of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

In this type of black hole attack has an internal spiteful node which fits in between the routes of given sender and receiver? As soon as it gets the chance this spiteful node make itself an active data route element. At the stage it is now able of conducting attack with the begin of data transmission.

External Black hole attack

External attacks stay outside of the network and deny access to network traffic or creating an excessive in network or by disordering the entire network. External attack can become a different kind of internal attack when it take control of internal spiteful node and control it to attack other nodes in MANET.

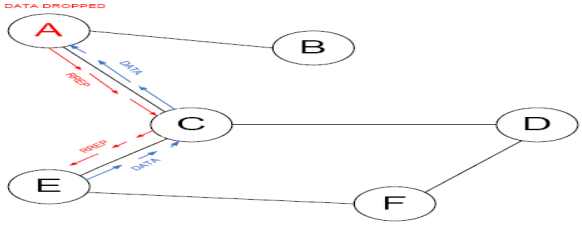

Fig. 4.2 Black hole attack specification

In AODV black hole attack the spiteful node "A" first detect the active route in between the sender "E" and host "D". The spiteful node "A" then send the RREP which contains the spoofed host 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".

5.PERFORMANCE ANALYSIS

This chapter explains the several performance metrics required for evaluation of protocols. To repeat the black hole attack, we starts with the overview of performance metrics that adds Host-to-Host delay, Throughput and Network load. In this matrix are uses because of it performance analysis of network.

5.1 Tool Simulations

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is a network and applications based software used for network management and analysis [18]. OPNET models connected devices, several protocols, architecture of various networks and technologies and provide simulations of their performances in virtual conditions.

5.2 Collection of Results and Statistics

Two types of statistics are involved in OPNET simulations. Global and object statistics, global statistics is for entire network's collections of data. Whereas object statistics involves separate node statistics. After the selection of statistics and running the simulations, result are taken and analyzed. In our case we have used by global discrete event statistics (DES).

5. 3 Simulation Setup

As shown in figure 5.1 employs the simulation arranges of a single scenario comprising of 32 mobile nodes moving at a constant speed of 100 meter per seconds. Total of 16 scenarios have been developed, all of them with mobility of 15 m/s. Number of nodes were varied and simulation time was taken 1000 sec. Simulation areas taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 14 Mbps with the default transmitting power of 0.01 watts. This spiteful node buffer size is lowered to a level which increases packet drop. In addition the simulation parameters are given in Table 5.1

Table 5.1

SIMULATION PARAMETERS	
Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	32 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	1000 seconds
Mobility (m/s)	100 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	22 Mbps
Mobility Model	Random waypoint

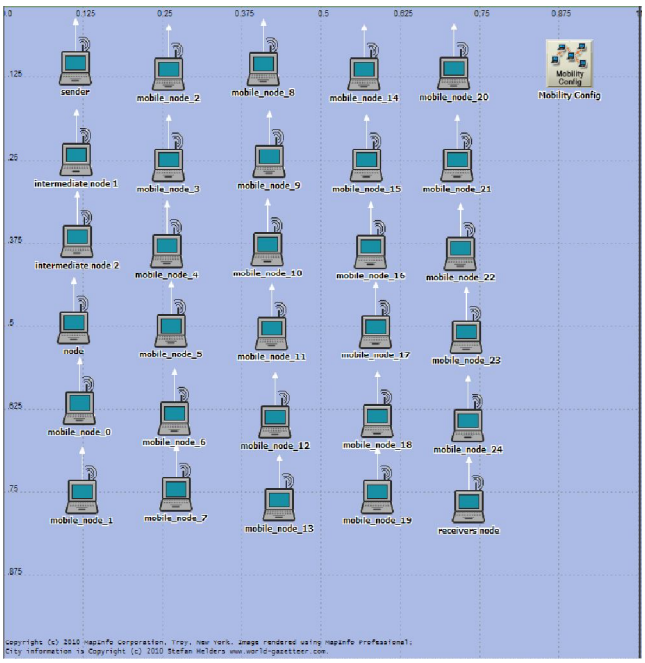

Fig.5.1 Simulation Environment for 30 nodes

6.RESULTS

In this result and its analysis based on the simulation performed in OPNET modeler 15.5. Our simulated results are provides in Figures (7.1-7.8) gives the variation in network nodes while under Black Hole attack. To determine the behavior of simulated intrusion based black hole attack, we studied the performance metrics of packet host-to-host delay, throughput and network load. These parameters are already defined in chapter 7 "performance analysis".

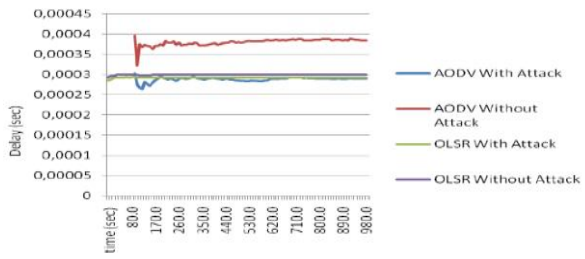

Fig. 1 Host-to-Host delays of OLSR and AODV with vs. Without attacks for 32 nodes

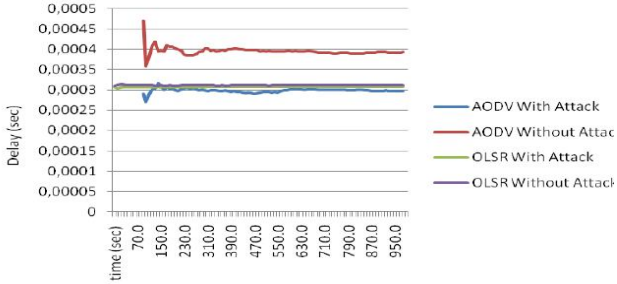

Fig. 2 Host-to-Host delays for OLSR and AODV with vs. Without attacks for 30 node

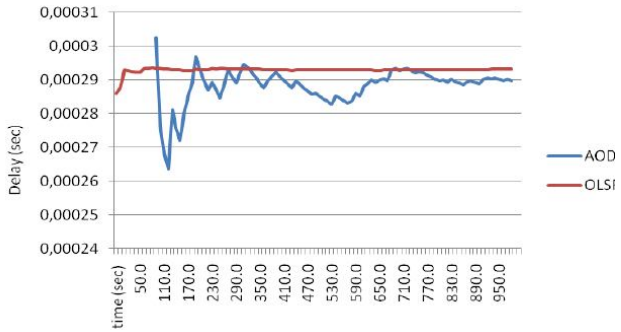

Fig. 3 Host-to-Host delays 16 nodes AODV vs. OLSR attacks

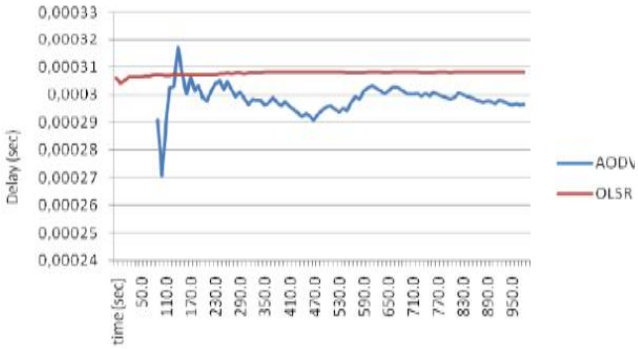

Fig. 4 Host-to-Host delays 30 node AODV vs. OLSR with Attacks

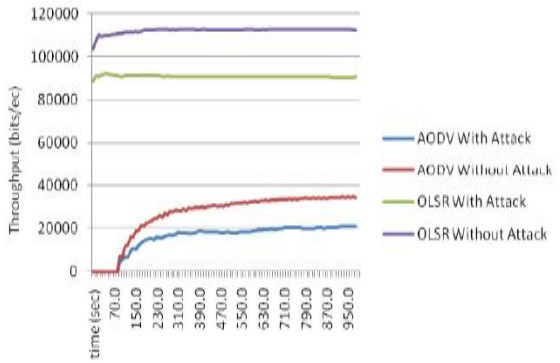

Fig. 5 Throughputs of OLSR and AODV with vs. without Attacks for 16 nodes

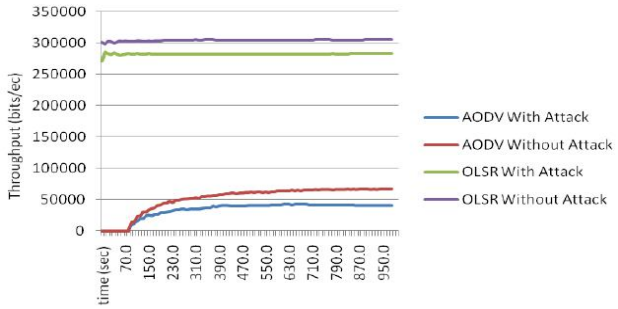

Fig. 6 Throughputs of OLSR and AODV with vs. without Attack for 30 nodes

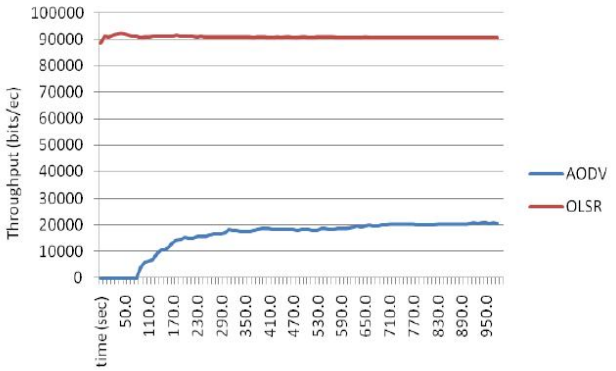

Fig. 7 Throughput 16 node AODV vs. OLSR with attacks

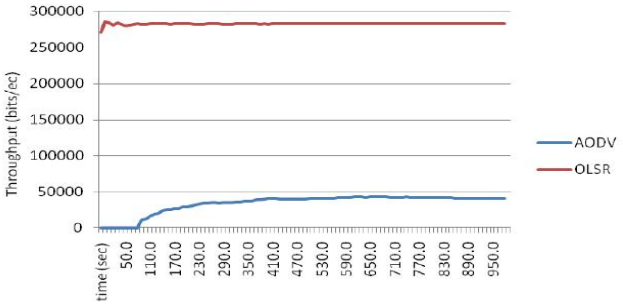

Fig. 8 Throughput 30 node AODV vs. OLSR with attacks

7. CONCLUSIONS & FUTURE WORK

MANETs has the ability to deploy a network where a traditional network an underlying base environment cannot possibly be deployed. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 10 to 20 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. An instance of network load in manner, there is effect on AODV by the spiteful node is less as compare to OLSR. Based on our research and analysis of simulation result we draw the conclusion that AODV is more susceptible to Black Hole attack than OLSR. These networks are exposed to both external and internal attacks as there is not centralized privacy mechanism. A lot of research work is required. There is a required to analyze Black Hole attack in other MANETs RPs such as DSR, TORA and GRP. Black Hole attack can be attack another way around i.e. as Sleep the act attack. The detection of this behavior of Black Hole attack as well as the remove strategy for such behavior has to be carried out for further research.

REFERENCES

[1] http://en.wikipedia.org/wiki/Personal_area_network, last visited 12, Apr, 2010.
[2] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.
[3] C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[4] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.
[5] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.
[6] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper,PAMPAS Workshop, Sept.16/17 2002.
[7] M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc Networks"
[8] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
[9] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".
[10] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in China, pp.366-370, Aug, 2007.
[11] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".
[12] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
[13] V.Mahajan, M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
[14] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr, 2006.
[15] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007
[16] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.
[17] Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date last viewed:2010-05-05
[18] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic"
[19] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-Hoc Networks," ACM Southeast Regional Conf. 2004.
[20] J. W. Creswell, Research Design: Qualitative, Quantitative and Mixed Methods Approach, 2nd Ed, Sage Publications Inc, California, July 2002.