Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Effects of Black Hole Attack on an AODV Routing Protocol Through the Using Opnet Simulator

Jasvinder
CSE Department, SBSSTC Ferozepur,
Punjab Technical University(Punjab), India

Monika Sachdeva
CSE Department, SBSSTC Ferozepur,
Punjab Technical University(Punjab), India

Abstract:-The growing popularity of wireless networks, and the peak in the present era, so as to attract the wireless user, regardless of their geographical location. There is more and more mobile ad hoc network (MANET) the risk of security threats. One of these security thread is Blackhole. In this type of attack a malicious node falsely advertised itself have a short and a fresh route to a destination and absorbs the all packets itself. In this paper we see the effect of black hole attack node under the AODV routing protocol . Protocols consider a comparative analysis of the black hole attack. Manet Black hole attack performance evaluation, agreements for exploration of the effects are more vulnerable to attack. Measurement of end-to-end throughput, latency and load optical network, packet loss. Simulation is done by the optimized network engineering tools (OPNET).

Keywords: MANET routing protocol and black hole attack, OPNET, AODV.

I. Introduction

Mobile ad hoc wireless network systems, self-governance and decentralization. MANET is free to move in the network and mobile nodes. Contract to participate in the network system or device (such as mobile phones, laptops, personal digital assistants, MP3 players and personal computers) and are mobiles, And these nodes that can act as a host / router, or both at the same time [1,2]. They can form in any network topology, depending on their relationship with each other. These nodes to configure their own ability, due to its self-configuration capabilities, they can be the urgent deployment of infrastructure without the need for any. Internet Engineering Task Force (IETF), is committed to developing an IP routing protocol for MANET Working Group (WG). Routing protocols challenging and exciting areas of research interest, the Many Routing Protocol have been developed , AODV, OLSR, DSR,GRP [18,19,20,21] etc.

In the mobile ad hoc network security is the basic concern for network functions work properly. This can be achieved network services available, and the confidentiality and integrity of data ensure that it has been met security issues. Often exposed to security attacks because of the open medium, dynamic topology, and the lack of central monitoring and management, and any cooperative algorithms and functions clear defense mechanism, such as the Declaration of the ad-hoc mobile networks. These factors may change the situation on the battlefield MANET security threats.

In Manet there is no any centralized administration and management, the nodes communicate with each other on the basis of mutual trust. This feature allows the ad hoc mobile networks within the network easier for an attacker to exploit. Wireless link also makes mobile ad hoc networks more vulnerable to attack, making it easier to attack the internal network, and access to ongoing contacts [11]. There can be a range of wireless link overhear a mobile node, or even participating in the network. MANET must be a safe way to transport and communications, mobile network attacks a growing threat, which is very difficult issues and important, Sound safe from today. In order to provide secure communications and transport, that the expert must understand the different types of network attacks. Sybil attack, Gray hole attack, Blackhole attacks, attack floods, directing attacks over the table, denial of service attacks (DoS), and misconduct of the contract selfishness, [3,4,5,6,7,8,9,10,15and 17]. MANET is open to these kinds of attacks, since the communication between nodes on the basis of mutual trust phenomenon. There is no central point for network management, and unauthorized facilities, and strongly change the topology and limited resources.

II. Review of the state of arts

The black hole in Manet involved in attacks is based on interactive routing protocols, such as allocated for consideration of adhoc on demand distance vector (AODV) and its impact has been described, pointing out that this attack is how to evaluate the performance of MANET. Very limited attention has been paid to the study of black hole attack in MANET using negative and positive influence of the two, and compares the two on the weakness of the attack. There is a need to address to attack both types of agreements, as well as in ad hoc wireless network attacks. This paper is an analysis of the black hole attack in MANET using AODV nature negative and active, respectively. Manet popular, despite the fact that these networks are heavily exposed to attacks [5,13,22]. MANET wireless link also makes the network more vulnerable to attack, making it easy for the attackers to enter the network and communications [5,12]. The attacks were analyzed Manet different impact on the network. MANET routing protocols are also being in the form of flooding, which is by the attacker or data through the use of flood RREQ of the attacker.

III. **Black Hole attack**

A black hole attack, a malicious node uses its routing protocol, in order to publicize that they have the shortest path to the destination node, and interest interceptor package [3,4,16,17], this notice of availability of fresh route in its way node, regardless of its routing checks tables. Therefore, the attacker always be the availability of the contract answering requests for guidance, and prevent it going to happen [12]. Flooding protocol based on malicious node receives responses from the actual request to respond, and so create a malicious forged routing. Once this road is built,whether now ignores all the other node reply [3,15]. Malicious nodes suitable for different ways of how to direct the data. A black hole problem, such as is shown in Figure 1, where the node "A" node "D" to send data packets, and begins the process of discovering the road. Therefore, if the node "C" is a malicious node, and will claim that it has a positive route to a specific destination, as long as the road receiving a request (RREQ) packet. It then sends the response to the node "A" in any other node. In this way, the node "A", that this is the path to take a positive initiative of the discovery of the way complete. Node "A" will ignore all other responses and will start planting package node "C". Thus, all of the lost packets will be consumed or lost.

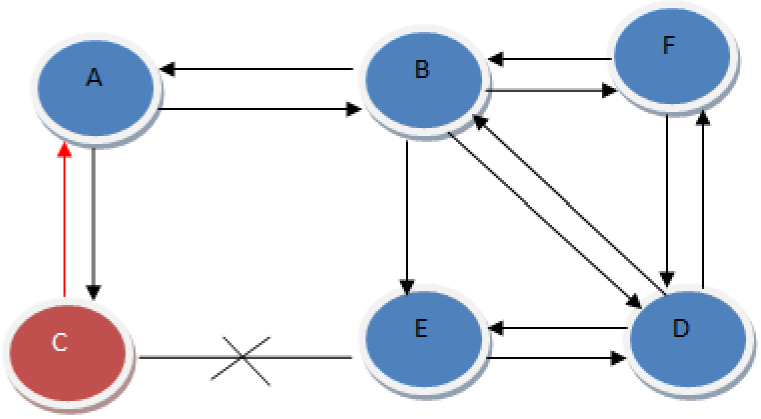

Fig 1 Black hole attack in AODV

IV. **Proposed Method**

Performance indicators that have been selected to evaluate the black hole attack packets end-to-end delay, throughput of the network and the network load, packet loss. Delay end-to-end package, and the average time needed to pass the package within the network. This includes everything from data packets that have been created from the sender, the receiver or the target until the data packet is received and the time in seconds. This includes the network, including the queue buffer, and the delay time caused by the transmission, the total delay of a route active.

The second parameter is productivity, which is from the sender to the time it takes the receiver can get the last packet of data to the receiver of the proportion of the total. It refers to the bid / Sec or packets / Sec. Changes in productivity Manet by various topologies, limited bandwidth and limited power. Connections are not adversely affected by a reliable parameter is one of the factors. The third parameter is the network load; it is to be accepted and queued for transmission of MAC layer has a higher total flow of the entire network. This indicates that the volume of traffic on the network. It represents the entire network in the recipient receiving layer to the top and the waiting list for the transfer of bits seconds total data traffic. It does not include any senior refused without waiting, due to the large volume of traffic data packets. The fourth parameter is the total packet loss, which shows the total packet loss during overall transmission from sender to the receiver end, with their distinct pause time with increasing order of the malicious node with each scenario.

The packet loss parameter indicates total loss of the packet between sender to the receiver under the black hole attacks. The tool used to stimulate research OPNET14.5. OPNET is a program on the Internet and a network management application and analysis [14]. OPNET model of communications equipment, and a different protocol, network architecture and the various technical, and provide an analog performance in a virtual environment. OPNET offers a variety of research and development solutions, which help the research of wireless technologies such as WI-Fi, WI-MAX, and UMTS, MANET protocol analysis and the analysis and design of improvements to enhance the core network technology, wireless sensor networks and provide energy management solutions. In this study, OPNET modeling node network, and determine the statistical data, and then run the simulation analysis results that were obtained. Figure 2 uses simulation node 45, 10 m / s at a constant speed of movement of the mobile node, including one scenario. There are 7 scenarios developed, all these mobility of 10 m / Sec. Changes in the number of nodes and the simulation time to take 1000 seconds. The time of the simulation for stable, in the first 300 seconds to simulate different then began to become stable, and the rest of the time. Simulation area is 1000 x 1000 m, which is enough to hold 45 to move freely, but not crowded. The second reason is that if we want to control the region, and the distance between each node and increase, and will introduce further delays due to the long distance between the nodes. Packet arrival time (seconds) and the size of the package (BITS) takes a pointer (1) Index (i.e 1024). Node 11 Mbps mobile data transfer rate is the default transfer of energy from 0.005 watts. Move selected random points at a uniform speed of 1 to 10 m / Sec, fixed pause time of 100,200,250 seconds. These data pause time, to reach the destination.

Our goal is to determine the protocol, which indicates that the black hole case of an attack, less weaknesses. AODV routing protocol, the protocol is negative and positive. AODV in case, is to reduce the size of the buffer to the level of malicious contract, which increases the data packets discarded, Table.1 architectural experiments.

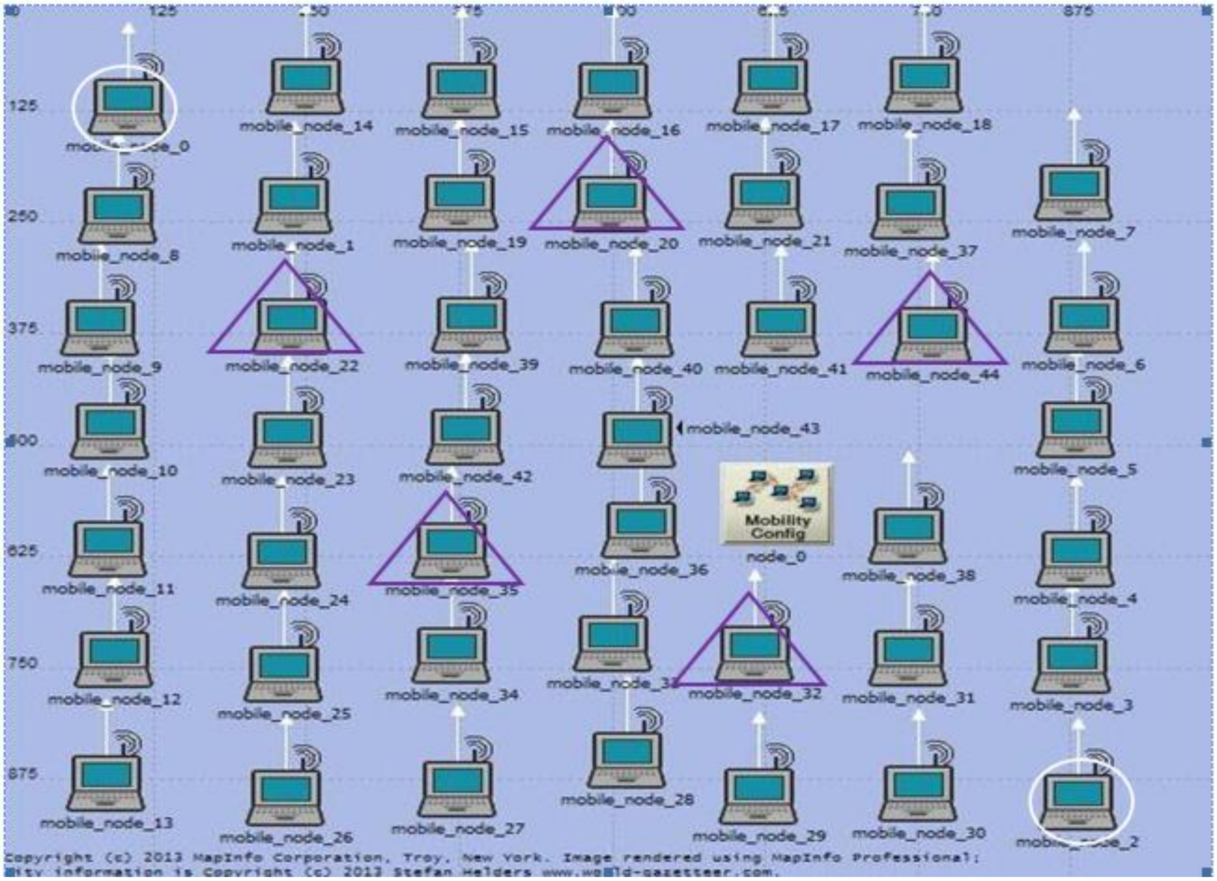

Fig. 2 Proposed Experimental Setup

Table.1 Simulation Parameters Simulation Parameters

Examination Protocols	AODV
Simulation Time	1000 sec.
Simulation area(m*m)	1000
Numbers of Nodes	45
Traffic Type	TCP
Performance Parameter	Throughput, Delay, Network load, Total Packets Loss
Pause time	100,200,250
Mobility	Uniform_int (0,10)
Packet size (bits)	Exponential (1024)
Transmit Power (w)	0.005
Data Rate (Mbps)	11 Mbps
Mobility model	Random Waypoint

Number of data source : Node 0
Number of data destination : Node2

To Create the Malicious environments, Five nodes are selected to launch the attack in different scenario with different pause time. The attack is launched separately with various numbers of malicious nodes.

Numbers of Malicious Node	Malicious Node Assignments	Pause time
1	Node 22	100
3	Node 22, Node 20, Node 35	200
5	Node 22, Node 20, Node 35, Node 32, Node 44	250

V. Results

If the attack of the black hole and without attack packets end-to-end delay depends on the routing protocol of the process and the number of nodes involved. Shown in Figure 3, the delay AODV node , in this case is the height (when there is no attack on the network node). This is due to the attack of the black hole, there is no need RREPs and RREQs packets sent malicious node package RREQ Send node to the destination node by reply having less delay . This increase in delay is due to the additional nodes through which then passes to the destination node However increase in the numbers of nodes also increases the difference of delay in AODV routing. The pause time values represent the movement of the objects. Each of the objects can move in a random direction, stop for some time (pause time), and then change its direction at random and move again.

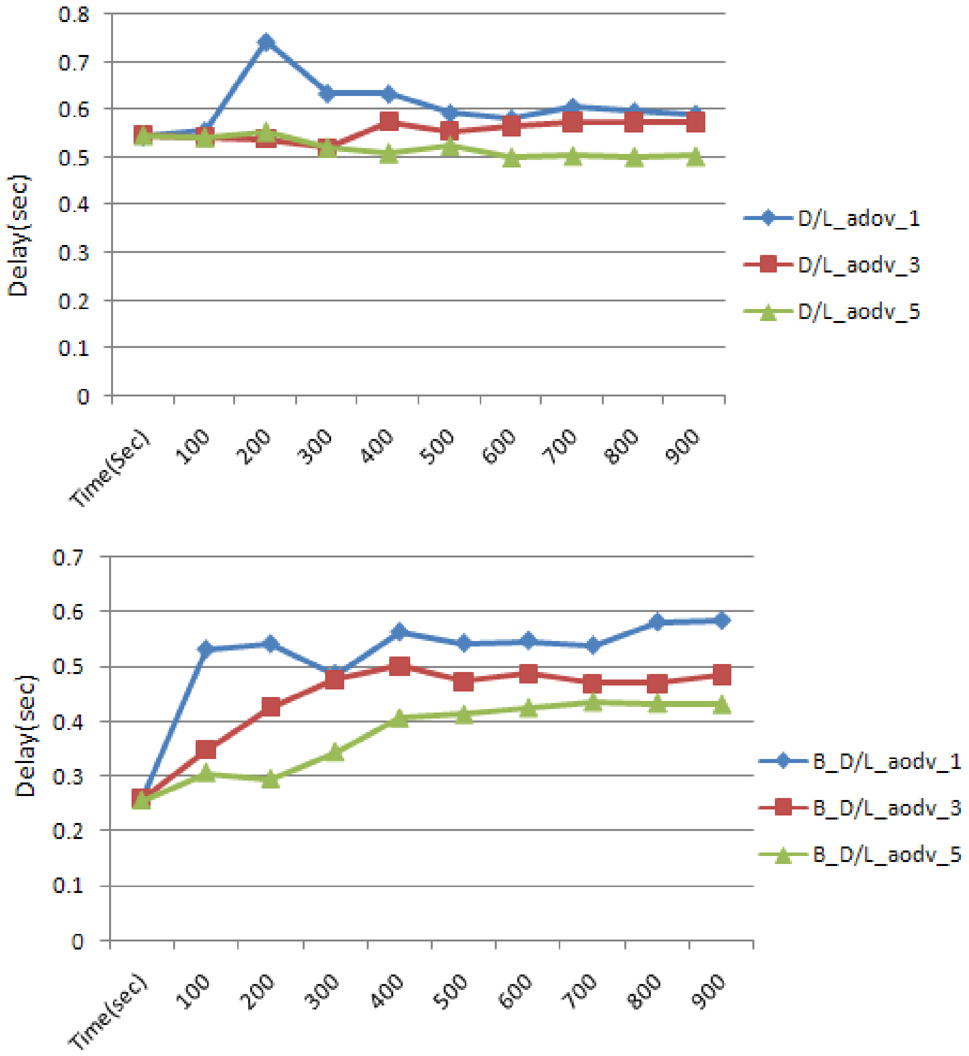

Fig. 3 End-to-end delay for AODV (with vs. without attack)

Figure 3 indicates the presence of malicious nodes, and the average delay end-to-end package. And you can see the shape Malicious Nodes, has a less latency AODV protocol . This is consistent, if the number is smaller than a decade. However, as noted increase in the number of nodes, and increase the delay AODV. In this figure shows the results of the black hole aodv and without attack with the respects of the different pause time as mention above. In AODV observed protocol in one case, an attack, which is higher than it was in the case of the before malicious glands because packets ignored the attacks.

Similarly, in Figure 4 throughput high due to the presence of a large number of nodes.

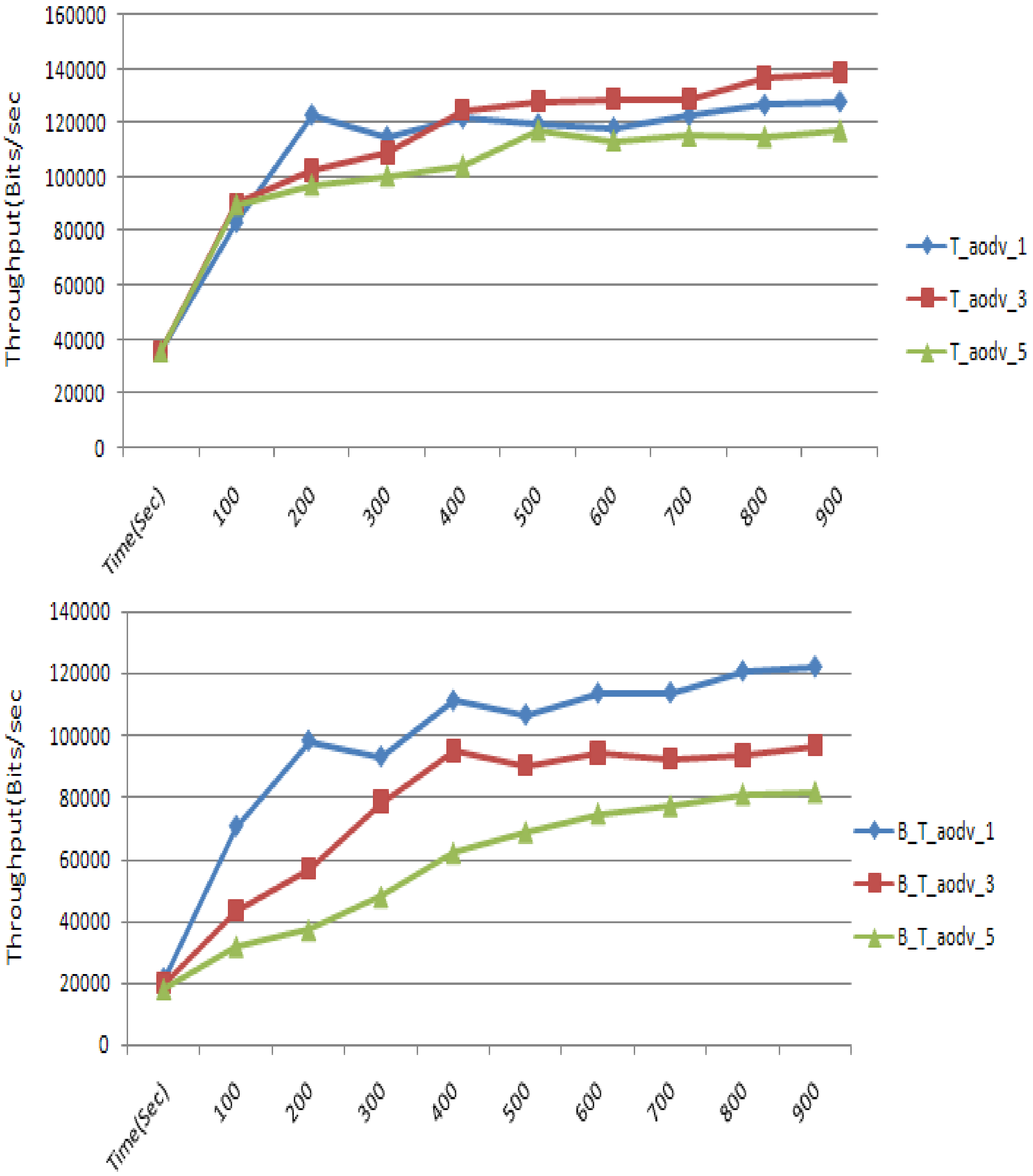

Fig. 4 Throughput for AODV (with vs. without attack)

Total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity. This is due to a decrease AODV routing response overall productivity. A malicious node sends a reply to track immediately and the data is sent to the malicious node which ignoring all the data. In the case of network load fig 5 : In the case of a larger number of nodes AODV react quickly. Start and stop and restart the node, so mobility after the start time, there is more stability, which makes the network load more pronounced. And are used widely ad hoc mobile ad network and the networks due to its flexible nature, and this is easy to deploy, regardless of geographical restrictions, in an environment of network infrastructure cannot be deployed traditional.

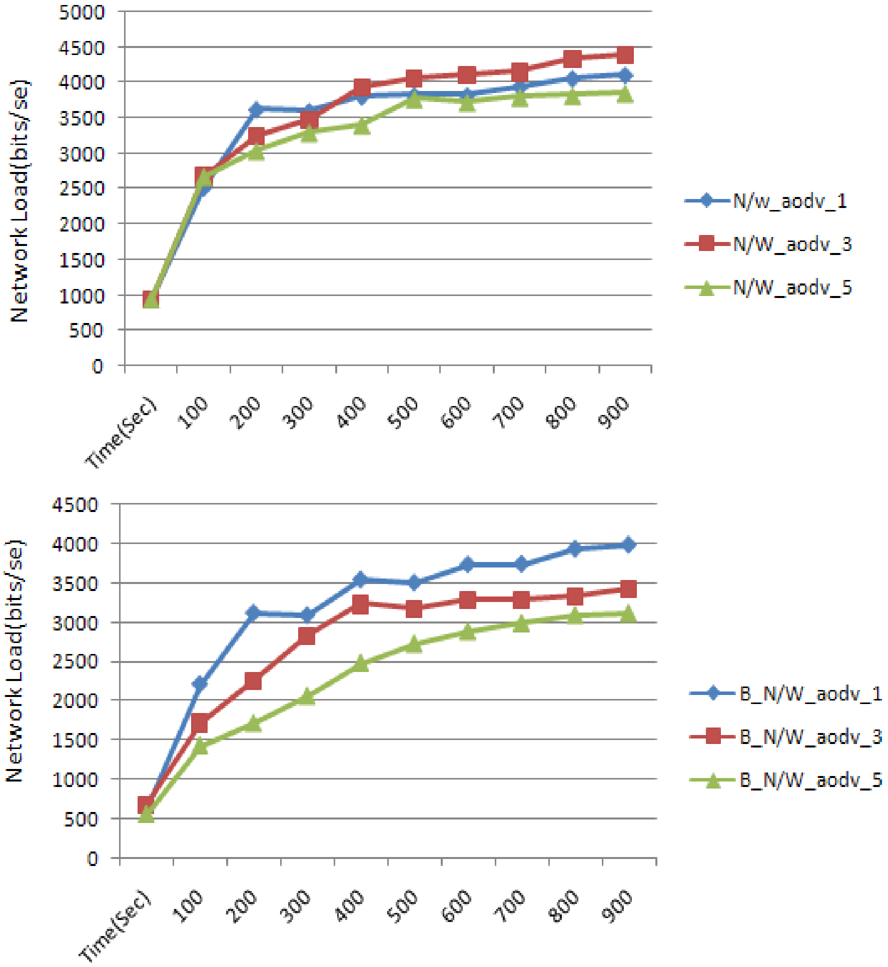

Fig. 5 Network Load in AODV (with vs. without attack)

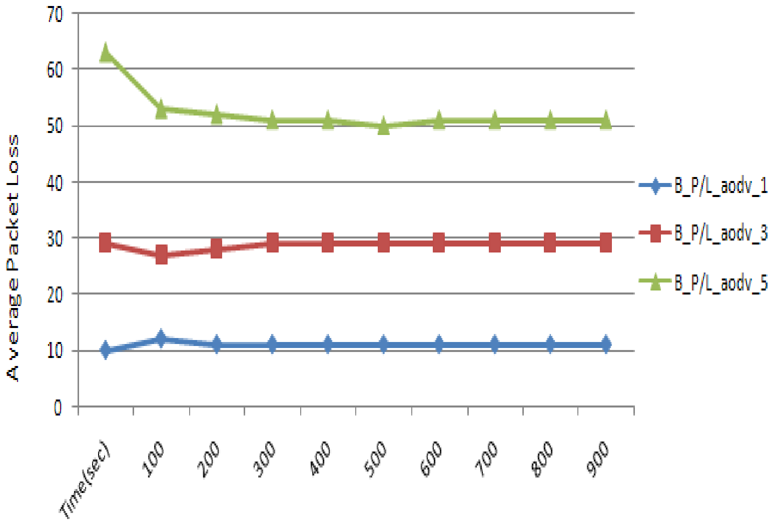

Fig 6: packets drop in aodv

This figure shows the losses of the packet from end to end transceiver . These are done with the help of five distinct malicious nodes. This figure shows that if only one malicious node then there is less packet drop compared with the five black hole nodes . It indicates if there is more black hole then packet drop is increasing and throughput decreases comparable to the normal transmission of aodv routing.

These networks are vulnerable to external and internal attacks, due to the lack of a centralized security mechanism. With the enormous potential importance for MANET comparison, it is still left to overcome the many challenges. Manet security is an important feature of the spread. In this paper, we analyze security threats custom mobile network and behavior challenges. Blackhole attack simulation and analysis of their impact on MANET have three bad matrix, and the ultimate goal to end the delay, network load and productivity. Results of simulation conducted in-depth analysis to draw definitive conclusions.

VI. Conclusion and future work

There are four different scenarios, packet drop and end-to-end delay, throughput and network performance standards parameters, and analysts believe that we attack the black hole. In the network protocol is a very important one for unnecessary efficiency, security and long-term. Protocols OLSR scored and doubled AODV survey. It was observed that when there is a larger number of nodes and more requests for guidance, it will affect the performance of the network. Delayed removal of the attack rate in the state of the Protocol AODV. However, the network load conditions, and there is more impact of the malicious AODV decade. Address the issue of the second search, the discovery of the ad hoc networks AODV is more affected by the attack, compared with the black hole attacks. The effort was discussed and analyzed in MANET using AODV protocol attacks five black holes. Needed to analyze the black hole attack other MANET routing protocols such as DSR, TORA and GRP. Other types of attacks, such as the gray hole, jellyfish and Siebel attack requires a comparative study of the black hole attack. They can be classified on the basis of how much they affect the performance of the network. Can attack Blackhole also attack the contrary, such as sleep deprivation attack. And is currently being considered in the research, as well as the strategy has been detected attack the black hole to eliminate this behavior such behavior.

References

1. C.M barushimana et. All. “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks,” Workshop on Advance Information Networking and Application, Vol. 2, 2003.
2. E. M. Royer et. All, “Ad-Hoc On Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop On Mobile Computing Systems and Applications, Feb, 1999.
3. B.Revathi et.all, “A Survey of Cooperative Black and Gray hole Attack in MANET,” International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012 ISSN 2278-733X.
4. Deepak KR T.V.P.Sundararajan,”An Immune Inspired Approach for Detecting Packet Drop Attacks in MANET” International Journal of Computer Applications (0975 – 8887) Volume 58– No.8, November 2012
5. Po-Wah Yau and Chris J. Mitchell,”Security Vulnerabilities in Ad Hoc Networks”. Mobile VCE Research Group Information Security Group Royal Holloway, University of London Egham, Surrey TW20 0EX, UK
6. Imad Aad Jean-Pierre Hubaux Edward W. Knightly,”Impact of Denial of Service Attacks on Ad Hoc Networks”, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.3839&rep=rep1&type=pdf
7. Jyoti Thaloret.all,” Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 2, February 2013 ISSN: 2277 128X
8. Gurjinder Kaur, Yogesh Chaba, V. K. Jain,“Distributed Denial of Service Attacks in Mobile Adhoc Networks”. World Academy of Science, Engineering and Technology 49 2011. http://www.waset.org/journals/waset/v49/v49-128.pdf.
9. V.Mahajan, M.Natue and A.Sethi, “Analysis of Wormhole Intrusion attacks in MANETs,” IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
10. 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
11. Wenjia Li and Anupam Joshi,”Security Issues in Mobile Ad Hoc Networks - A Survey. http://www.csee.umbc.edu /~wenjia1/ 699_report.pdf.
12. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006
13. F. Maan, Y. Abbas, N. Mazhar,”Vulnerability Assessment of AODV and SAODV RoutingProtocols Against Network Routing Attacks andPerformance Comparisons. http://www.academia.edu/ 1575115/Vulnerability_assessment_ of_AODV_and_SAODV_routing_protocols_against_network_routing_attacks_and_performance_comparisons
14. Opnet Technologies, Inc. “Opnet Simulator,” [Online]. Available: www.opnet.com, [Accessed: March. 10, 2013].
15. Mieso K. Denko,”Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme.” http://rise.cse.iitm.ac.in/wiki/images/3/35/Rep5.pdf
16. S.Sharma, Rajshree, R.P.Pandey, V.Shukla, “Bluff-Probe Based Black Hole Node Detection and Prevention, ”IEEE International Advance Computing Conference” (IACC 2009), pp. 458-462, March, 2009.

17. Irshad Ullah et. all, "Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2012 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org
18. C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: "http://www. faqs.org / rfcs/rfc3561.html". [Accessed: February. 11, 2011]
19. T.Clausen, P.Jacquet , "Optimized Link State Routing Protocol (OLSR),"October, 2003, [Online]. Available: http://www .faqs.org/rfcs/rfc3626.html. [Accessed: April. 10, 2012].
20. D. Johnson,"T he Dynamic Source Routing Protocol (DSR)for Mobile Ad Hoc Networks for IPv4." Feburary,2007,[online]. Available : http://tools.ietf.org/html/rfc4728.html.
21. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009
22. Abhishek Gupta,"Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model." International Journal of Computer Applications (0975 – 8887) Volume 57– No.12, November 2012