Performance Analysis of AODV in presence of Attacks

BHAWNA SINGLA[1], A.K.VERMA[2], L.R.RAHEJA[3]
[1]Tharap University, Patiala, INDIA [2]Indian institute of Technology, Kharagpur, INDIA
[1]bhawna_singla@yahoo.com, [2]akverma@thapar.com, [3]lrr_2004@yahoo.com

Abstract:-Mobile Adhoc Network (MANET) is a combination of three words mobile means that are able to change their position + adhoc means temporary and network means autonomous collection of nodes. MANET is the subcategory of wireless network i.e. collection of nodes over wireless communication medium where all the node are capable to change their position so that topology of network keeps on changing. Routing protocol determines the route from source node to destination node. Adhoc on demand distance vector (AODV) routing protocol is a type of reactive routing protocol that determines the route whenever there is a requirement. However MANETs are vulnerable to number of attacks due to such as lack of centralized infrastructure, wireless medium and dynamic topology. In general, attacks can be categorized as active attack and passive attack depending on whether it's intention is to monitor the traffic or to cause damage to the network. Specifically, in this paper blackhole attack , wormhole attack and selfish node attack are being observed on AODV routing protocol. Selfish node attack is caused by selfish node that selfishly stops forwarding of packet and blackhole and wormhole attacks are caused by malicious node. This paper presents introduction of all these attacks and then it analyzes the performance of AODV under these attacks. The comparative analysis of these attacks is done with the help of NS2 simulation in terms of: cumulative sum of packets, throughput, end-to-end delay. The packet Ids of all the dropped packets are also plotted. Moreover, optimal packet size for the maximum throughput is also observed.

Key-words: AODV, blackhole, wormhole, selfish, throughput, end-to-end delay, packet size

1 Introduction

This paper considers AODV as the basic routing protocol for its study. AODV is an on demand reactive routing protocol that determines the route from source to destination whenever there is a requirement. The working of AODV protocol can be divided into two phases : Route Discovery and Route Maintenance [1].

Route Discovery [2,3]: In route discovery phase, every node maintains a table regarding its neighbor with respect to metric such as distance or number of hops etc. Determination of neighbor is done with the help of HELLO message. HELLO message is broadcasted by every node at regular time intervals. Whenever there is a route requirement source node broadcasts a special type of control message called Route Request message (RREQ) to its neighbor. RREQ control packet contains the several fields like destination address of node, destination sequence number, broadcast ID etc. Whenever intermediate node receives a new broadcast RREQ then the following cases may occur.

a) That node may be the destination node or it may be the intermediate node that contains the fresh path to the destination. If it is the case, then sequence number of the packet is checked against the destination sequence number for calculating the path freshness. If it is the fresh path then Route Reply message (RREP) is generated which is sent back to the source node to calculate the path.
b) That node does not have the route through itself. In that case it rebroadcast RREQ from itself where all the field values remains same instead of IP address. The IP address

is replaced with IP address of the intermediate node.

Route Maintenance: Maintenance of routes is done with the help of HELLO messages which is a special type of RREP with hopcount =0.These HELLO messages are broadcasted periodically to the immediate neighbors. If neighbor receives the HELLO message that means the node is still active otherwise the neighbor may assume that the link is broken.

1.1 **Attacks**

Due to vulnerability of MANETs such as lack of centralized infrastructure, common wireless communication media, dynamic topology etc., MANETs are vulnerable to number of attacks. In context of network, attack can be described as action taken against the target with the intention of doing harm. Attacks in MANETs can be divided in groups of (i) active and passive attack and (ii) external and internal attack. In the first classification, Passive attack keeps track of the data in the communication without disrupting the operation. It typically involves only eavesdropping of data or making node to not participate in the communication. Examples of passive attack include traffic analysis, selfish node attack etc. Whereas active attacks causes disruption of information for example replication, modification and deletion of data. Depending on t he classification, nodes can also be categorized into two groups[4]

c) Selfish node: These nodes do not intend to harm the system however their aim is to save its resources to maximum. These nodes may refuse to cooperate by discarding all incoming packet (control and data) except those which are destined to them.

d) Malicious node: do not aim to reserve the resources rather they try to participate in the conversation more and more by sabotaging other nodes and do harm to conversation.

However, in second classification, External attacks[5] are due to outside nodes while internal attacks are from nodes that belong to the network and have become compromised.

This paper considers three attacks –Blackhole, Wormhole and selfish node attack on A ODV routing protocol where blackhole attack and wormhole attack is an example of malicious node attack and selfish node attack is example of selfish node attack. These three attacks are chosen so as to see the impact of malicious node and selfish node on the AODV routing protocol. Further, in section 3 the attacks are implemented using NS-2 simulator and the results are presented showing performance of AODV routing protocol under the presence of these attack.

2 Review of Attacks

2.1 **Selfish Node Attack**

As stated earlier, selfish node do not forward the packet with the intend of saving its resources[6,7,8,9,10,11,12,13].

2.2 **Blackhole Attack**

In blackhole attack, malicious node advertises itself as having the shortest path. So that maximum traffic is diverted through itself but afterwards drops the packets (data as well as control packet)[14,15,16,17,18,19,20,21].

2.3 **Wormhole Attack**

In wormhole attack, malicious node tries to establish a direct one hop l ink between two far points in the network. Malicious node tunnels all the traffic through the link to the other point instead of using multiple hops for communication.[24,25,26,27,28,29]

3 Experimental Setup

This paper uses NS-2.34 [30] for implementation on UBUNTU 10.04 platform. AODV protocol simulation, part of the simulator, is the routing protocol. For selfish and misbehaving nodes, a modified version of AODV was developed. Specifically, selfish node donot forward data packets and blackhole node drops all the packet and wormhole nodes forward the entire packet through wormhole link. The results are then compared to see the impact of attacks on AODV routing protocol. The default network parameters are depicted in table 1. This analysis is done in terms of (a) cumulative sum of number of packet, (b) throughput, (c) packet size vs throughput of packet, (d) packet ids of dropped and sent packet, (e) end- to-end delay

3.1. Cumulative sum of packets: Cumulative sum is the sequence of partial sums of a given sequence where a partial sum of first N terms in a seq uence $(a_k)^n{}_{k=1}$ is given by

$$S_N = \sum_{k=1}^{N} a_k$$

For example, cumulative sum of the sequence {a,b,c,…..} are a, a+b, a+b+c,….. In our simulation, cumulative sum of dropped packet at all nodes and cumulative sum of number of packet at malicious or selfish node is considered so as to see percentage of harm it makes to the current routing protocol.

3.2. Throughput of packet Vs simulation time: Throughput is defined as ratio of received packet and sent packet per unit of time which can be which can also be expressed as

$T = \frac{P_r/P_s}{T}$ where Pr is the total number of received packet at the destination, Ps is the packet send by the source and T is the time taken. Greater the value of the throughput means better the performance of the protocol. In this paper, throughput of sending and dropped packets are compared.

3.3. Packet Id: is the unique ID given to control and data packets. One can also keep track of Id's of dropped and sent packet.

3.4. Packet Size Vs average throughput: helps us in determining optimal value of packet size which results in highest throughput. It can also help in determining maximum packet overhead that network can bear.

3.5. End-to-end delay: is the average time taken by packet to arrive to the destination after it starts from the source. Lower the value of delay, better is the protocol

$$\sum(arrivetime - send\ time)/\sum number\ of\ connections$$

We consider a network of nodes placed in various arrangements (one source and one destination and the remaining being intermediate node) within a 1500m X 1500m area. The simulation lasts up to 8.0 sec.

Table 1: Simulation Parameters used in the comparison

Area	1500*1500 m	Antenna Model	Omniantenna
Simulation time	8 sec	Traffic	CBR
Nodes	20	Packet size	28 bytes
Nodes Placement	Grid	MAC layer	802.11
Pathloss model	Two ray	Maximum packet size in IFQ	1000
Interface queue type	Droptrail	Transmission range	250m

4 Results

4.1 Selfish node Attack : As shown in figure 7, firstly cumulative sum of number of total dropped packet in the network, dropped packet at the selfish node 9, total sent packet is compared and it is seen that they keeps on linearly increasing with send event time. However, cumulative sum of dropped packet at the selfish node is much lesser than cumulative sum of total number of dropped packet. Thus, selfish node functioning is not merely restricted to dropping of packet, rather it's sole purpose is not to forward the data or control packet selfishly (e.g. to save resources such as battery life or CPU cycles etc.). Selfish behavior of the node also affects the throughput of sending packet and dropping packet as shown in figure 8,9. When the selfish node acts selfishly, the throughput of sending packet becomes lesser than throughput of dropped packet. Packet ID's of the entire dropped packet, dropped packet at the node 9, sent packet is also plotted in the figure 10. Throughput of a node also depends on the packet size as shown in figure 11. In this selfish node attack, maximal value of throughput is taken for the packet size of 1032 bytes. Further end-to-end delay is also plotted in terms of send time. The selfish node attack does not effects much the end-to end- delay as shown in figure 12.

4.2 Blackhole Attack: Performance matrices of the blackhole attack is compared in the figure 13. In this case also cumulative sum of number of total dropped packet in the network, dropped packet at the blackhole node 6, total sent packet increases linearly. However, cumulative sum of dropped packet at the blackhole node is comparable to cumulative sum of total number of dropped packet. This is because blackhole node sole purpose is to drop all the packets which are directed to it. Thus, major part of dropping is constituted by blackhole node. Blackhole behavior of the node also affects the throughput as shown in figure 14,15 of sending packet and dropping packet. In this case throughput of dropped packet is much larger than throughput of sending packet. Packet ID's of the entire dropped packet, dropped packet at the node 6, sent packet is also plotted in the figure 16. In blackhole node attack, maximal value of throughput is taken for the packet size of 1032 bytes. Further end-to-end delay, as shown in the figure 18, is not much affected by blackhole attack.

4.3 Wormhole Attack: Performance matrices of the Wormhole attack is compared in the figure 19. In this case malicious node is not merely restricted to dropping of packet rather it is more concerned about forwarding the packet to the wormhole link having low latency. This is the main reason for less percentage of dropped packets at the wormhole node. However, throughput of dropped packet as shown in figure 20 is comparable to throughput of sending packet. Packet ID's of the entire dropped packet, dropped packet at the malicious node node 9 a nd 6, sent packet is also plotted in the figure 21. In wormhole attack, maximal value of throughput is taken for the packet size of 1032 bytes. Further end-to-end delay is also shown in the figure 23.

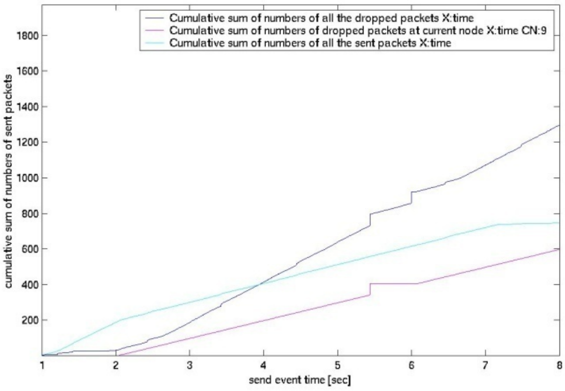


Figure 7 : Cumulative sum of packets comparison vs send event time in selfish node attack

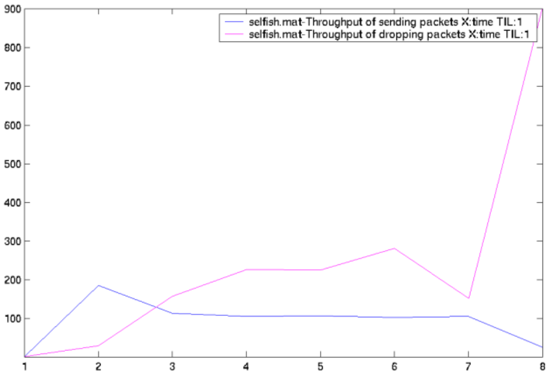


Figure 8 : Throughput comparison in selfish node attack

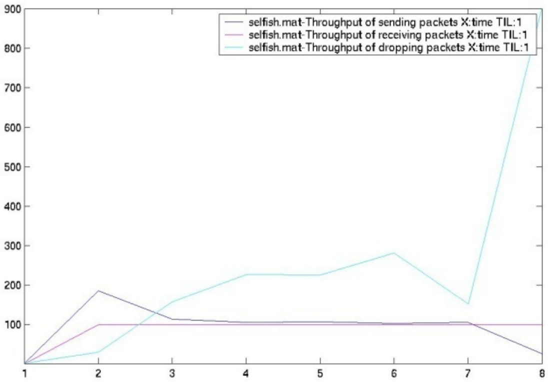


Figure 9 : Throughput of sending, Dropping and receiving packet in selfish node attack

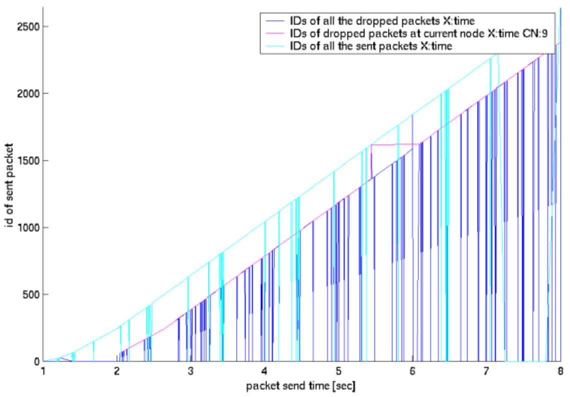


Figure 10 : Packet IDs in selfish node attack

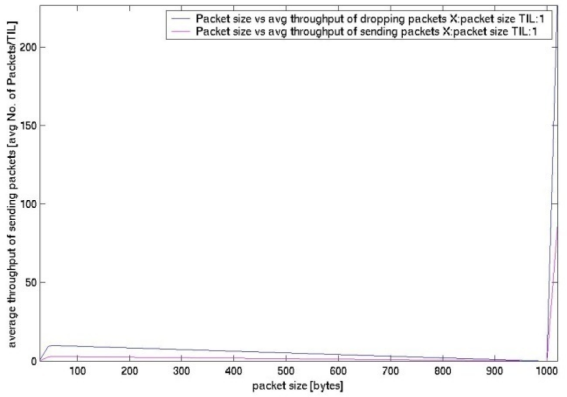


Figure 11: Packet size in selfish node attack

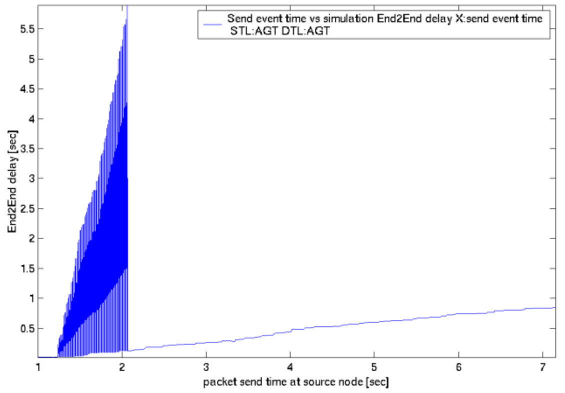


Figure 12: End-to end delay in selfish node attack

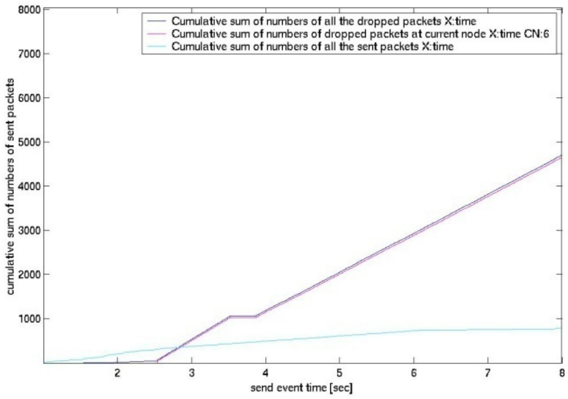


Figure 13: Cumulative sum of packets comparison vs send event time in Blackhole attack

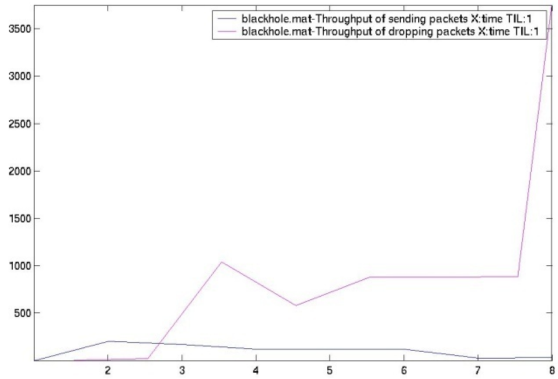


Figure 14: Throughput comparison in Blackhole attack

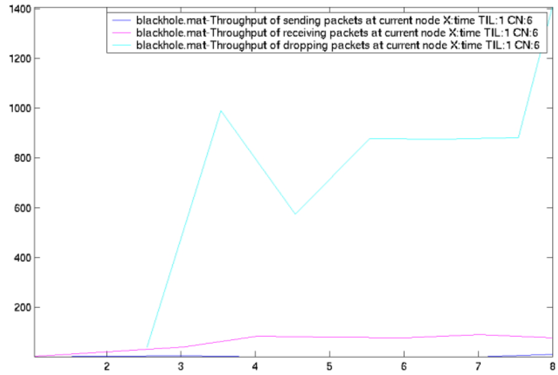


Figure 15: Throughput of sending, Dropping and receiving packet in Blackhole attack

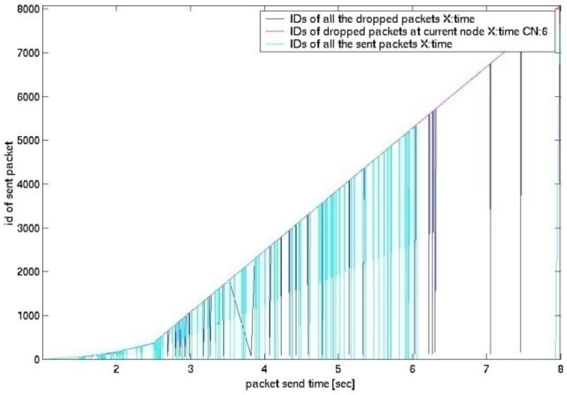


Figure 16 : Packet IDs in Blackhole attack

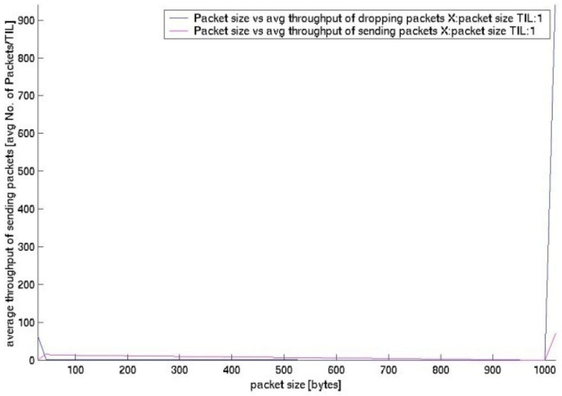


Figure 17: Packet size in Blackhole attack

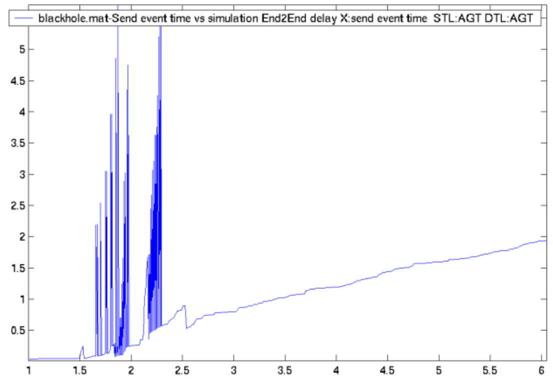
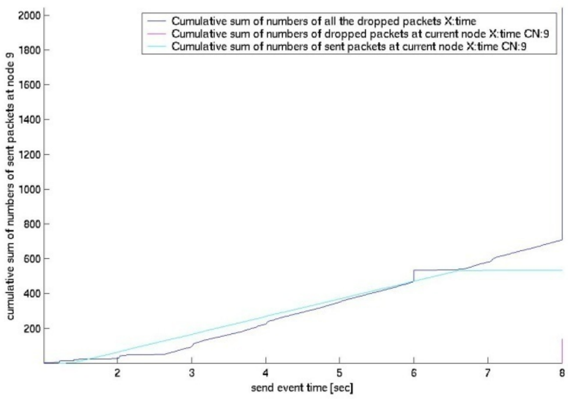


Figure 18: End-to end delay in Blackhole attack



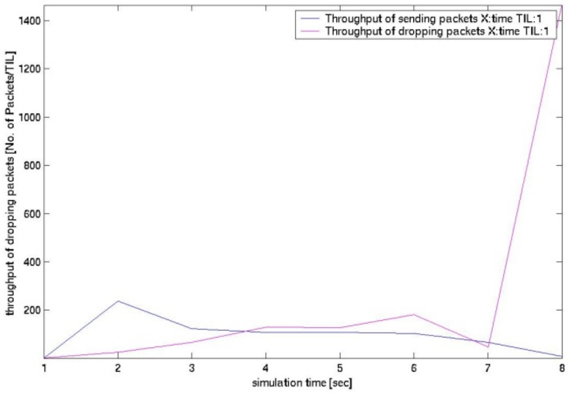


Figure 19: Cumulative sum of packets comparison vs send event time in Wormhole attack

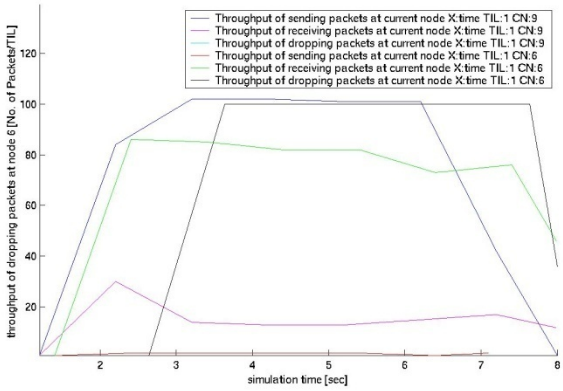


Figure 20 : Throughput of sending, Dropping and receiving packet in Wormhole attack

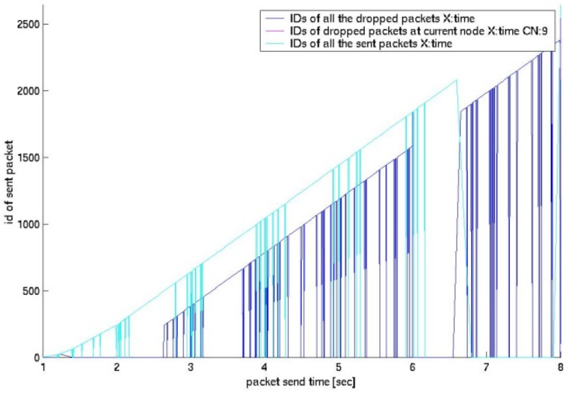


Figure 21 : Packet IDs in Wormhole attack

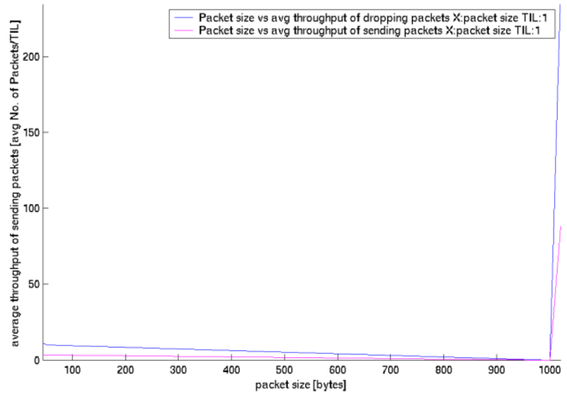


Figure 22: Packet size in wormhole attack

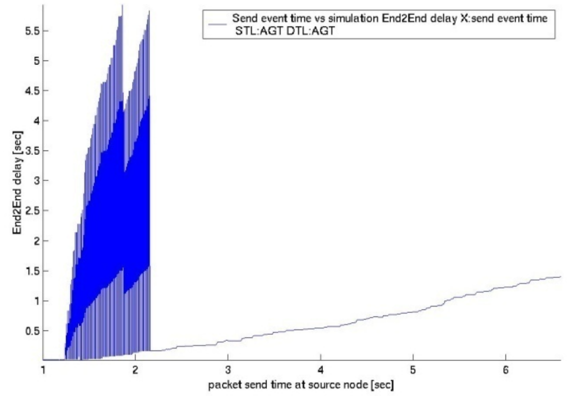


Figure 23: End-to end delay in Wormhole attack

5 Conclusion

This paper presents the working of AODV in presence of selfish node and malicious node attack (blackhole and wormhole attack). According to the definition of malicious node, its main intention is to cause damage to the network .Therefore, throughput of dropped packet increases sharply. However the selfish node attack is interested in saving of resources therefore throughput of dropped packet is least affected but throughput of the forwarding packet decreases when it stops forwarding the packet. However both of these attacks have negligible effect on end-to-end delay. AODV gives maximum throughput for the packet size of 1032 bytes irrespective of any attack. This paper focuses on implementation of three major attack that are very much dangerous and need major attention. The attacks can be understood by studying how it affects the routing protocol. This paper presents an indepth analysis of attacks by implementing under NS2.34 simulator. This work may be used in future to understand the working of attack and further to invent the solution against these attacks. This work may also be used to develop an architecture that aims not only as a so lution to single attack rather series of attack that have common functionality.

References:

[1]. Perkins, E. Royer , “ Adhoc On-demand Distance Vector Routing”, Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 99–100, 1999

[2]. Deyu Lin , “Optimization and Realization of Adhoc On-Demand Distance Vector Routing Based on NS2”, Proceedings of First Information Computing and Applications , pp. 531-537, 2012

[3]. Bhawna Singla, A.K.Verma, L.R.Raheja, “Performance of AODV under different scale network”, Wulfenia , volume 20, no.3, March2013

[4]. Deng H, Li W, D.P. Agarwal, “Routing Security in Wireless Ad-hoc Networks” IEEE Communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859

[5]. B. Wu et al., “A Survey of Attacks and Countermeasures in Mobile Adhoc Networks,” Wireless/Mobile NetworkSecurity, Springer, volume 17, 2006.

[6]. Jerzy Konarski, “Selfishness Detection in Mobile Adhoc Networks: How Dissemination of Indirect Information Turns into a Strategic Issue”, Proceedings of the 2nd International Conference on Information Technology, ICIT

2010 , 28-30 June 2010

[7]. Kumar, Jebakumar Mohan Singh Pappaji Josh, et al. "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT." *EURASIP Journal on Wireless Communications and Networking* 2015.1 (2015): 1-11.

[8]. Subramaniyan, Senthilkumar, William Johnson, and Karthikeyan Subramaniyan. "A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique." *EURASIP Journal on Wireless Communications and Networking* 2014.1 (2014): 205.

[9]. Kumar, Amit, Vijay K. Katiyar, and Kamal Kumar. "A Purely Localized Random Key Sequencing Using Accelerated Hashing in Wireless Ad-Hoc Networks." *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications*. Springer, Singapore, 2017.

[10]. Duan, Junqi, et al. "TSRF: A trust-aware secure routing framework in wireless sensor networks." *International Journal of Distributed Sensor Networks* 2014 (2014).

[11]. Das, Debjit, Koushik Majumder, and Anurag Dasgupta. "Selfish node detection and low cost data transmission in MANET using game theory." *Procedia Computer Science* 54 (2015): 92-101.

[12]. Shah, Sachi N., and Rutvij H. Jhaveri. "A survey oj various approaches to detect selfishness in wireless ad-hoc networks." *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*. IEEE, 2015.

[13]. Y. Yoo and D. P. Agrawal, “Why does it pay to be selfish in a MANET?,” *IEEE Wireless Communications Magazine*, vol. 13, issue 6, pp. 87-97, Dec. 2006

[14]. Raja Mahmood RA, Khan AI , “A Survey on Detecting Blackhole Attack in AODV-based Mobile Adhoc Networks.” Proceedings of International Symposium on H igh Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007

[15]. Saini A, Kumar H , “ Comparison between Various Blackhole Detection Techniques in MANET” Proceedings of National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010

[16]. Bar, Radha Krishna, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh. "QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack." *Procedia Technology* 10 (2013): 530-537.

[17]. Lo, Nai-Wei, and Fang-Ling Liu. "A secure routing protocol to prevent cooperative black hole attack in MANET." *Intelligent Technologies and Engineering Systems*. Springer New York, 2013. 59-65.

[18]. Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[19]. [15] Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6

[20]. [16] Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[21]. [17]. Raj PN, Swadas PB (2009) DPRAODV: A Dy namic Learning System Against Blackhole Attack in AODV based MANET.International Journal of Computer Science 2:54–59. doi: abs/0909.2371

[22]. [18] Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010.

[23]. [19] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010

[24]. L.Hu and D.Evans, “ Using directional antennas to prevent against wormhole attacks”, Proceedings of NDSS Feb.2004

[25]. Y.Hu, A.Perrigand D. Johnson, “Packet leashes : A defense against wormhole attack in Wireless network”, Proceedings of INFOCOM ,volume 2, April 2003

[26]. R.Poovendran and L.Lazos, “A graph theoretic framework for preventing wormhole attacks in wireless adhoc networks” Wireless networks, volume 13, no.1 , pp.27-59, 2007

[27]. Shrivastava, Akansha, and Rajni Dubey. "Wormhole Attack in Mobile Ad-hoc Network: A Survey." *International Journal of Security and Its Applications* 9.7 (2015): 293-298.

[28]. Ji, Shiyu, Tingting Chen, and Sheng Zhong. "Wormhole attack detection algorithms in wireless network coding systems." *IEEE Transactions on Mobile Computing* 14.3 (2015): 660-674.

[29]. Biswas, Juhi, Ajay Gupta, and Dayashankar Singh. "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol." *Industrial and Information Systems (ICIIS), 2014 9th International Conference on*. IEEE, 2014.

[30]. K. Fall and K.Varadhan, “The NS Mannual”, available at http://www.isi.edu/nsnam/ns.