Analysis of security attacks on AODV routing

Abdelshafy, M. & King, P. J. B.

Original citation & hyperlink:
Abdelshafy, M & King, PJB 2013, Analysis of security attacks on AODV routing. in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013) . IEEE, pp. 290-295, 8th International Conference for Internet Technology and Secured Transactions, London, United Kingdom, 9/12/13.
https://dx.doi.org/10.1109/ICITST.2013.6750209

DOI 10.1109/ICITST.2013.6750209
ISBN 978-1-908320-20-9

Publisher: IEEE

Analysis of Security Attacks on AODV Routing

Mohamed A. Abdelshafy
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: ma814@hw.ac.uk

Peter J. B. King
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: P.J.B.King@hw.ac.uk

***Abstract*—MANET routing protocols have many vulnerabilities that may be exploited by malicious nodes to disrupt the normal routing behavior. In this paper, we present a vulnerability analysis of AODV. We simulate four routing attacks to analyse their impacts on AODV protocol using NS-2 network simulator. These attacks are blackhole, grayhole, selfish and flooding attacks. The blackhole and flooding attacks have a severe impact on the network performance while the selfish and grayhole attacks have less significant effect on the network performance.**

I. Introduction

A Mobile Ad Hoc Network (MANET) is a decentralized infrastructureless network in which nodes cooperate to forward data from a source to a destination. Each node in a MANET acts both as a router and as a host.

Several routing protocols have been designed for MANETs [3] to optimize network routing performance over the past years. The major issues involved in designing a routing protocol for MANET are nodes mobility, bandwidth constrained and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology.

MANET routing protocols can be classified as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. While in reactive (on-demand) routing protocols, routes are created whenever a source requires to send data to a destination node which means that these protocols are initiated by a source on-demand. In this paper, we concentrate on the AODV protocol [10]. AODV is a reactive protocol, chosen by the IETF for standardization, which has been extensively studied.

Conventional MANET routing protocols assume that all nodes cooperate without maliciously disrupting the operation of the protocol and do not provide defense against malicious attackers. However, the existence of malicious nodes cannot be ignored in computer networks, especially in MANETs because of the wireless nature of the network. MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself [6] due its characteristics. Nodes in MANET have limited computation and power capabilities that make the network more vulnerable to Denial of Service (DoS) attacks. It is difficult to implement cryptography and key management algorithms which need high computations like public key algorithms. Node mobility introduces also a difficulty of distinguishing between stale routes and fake routes. A malicious node can attack the network layer in MANET either by not forwarding packets or by changing some parameters of routing messages such as sequence number and IP addresses, sending fake messages several times and sending fake routing information to disrupt routing operations. There are a large number of existing attacks against MANET [12] and solutions to these attacks. Simulation and study of such attacks [9] [13] has become necessary in order to provide defence mechanisms against these types of attacks.

The rest of the paper is organized as follows. In section II, an overview of the AODV routing protocol is presented and the impact of some attacks on MANET is discussed. In section III, the simulation parameters and results are given. In section IV concluding remarks are introduced.

II. AODV Protocol and Security Flaws

Ad Hoc On-Demand Vector Routing (AODV) [10] is a reactive routing protocol. It uses destination sequence numbers to ensure the freshness of routes and guarantee loop freedom. To find a path to a destination, a node broadcasts a route request (RREQ) packet to its neighbors using a new sequence number. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ unless it has a fresher one. When the intended destination or an intermediate node that has a fresh route to the destination receives the RREQ, it unicasts a reply by sending a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. Then the source node starts sending data packets to the destination node through the neighboring node that first responded with an RREP. When an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate a route error (RERR) packet to each of its active upstream neighbors. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deal with data transmission. This scenario decreases the memory overhead, minimizes the use of network resources, and runs well in high mobility situation.

The behavior of a malicious node is to disrupt the operation of the AODV routing protocol [6]. The malicious node can spoof source or destination IP address, modify RREQ or RREP packets and/or generate fake RREP or RERR packets. Some of the attacks such as blackhole and grayhole attack are discovered by the source node in connection-oriented protocols such as TCP because the lack of acknowledgments. The source node understands that there is a link error because the destination node does not send ACK packets. If the source

node sends out UDP data packets the problem is not detected because UDP is a connectionless protocol.

A. Flooding Attack on AODV

In a flooding attack [5], a malicious node takes advantage of the route discovery process of the AODV routing protocol. The malicious node aims to flood the network with a large number of RREQs to non-existent destinations in the network which takes a lot of the network resources. Since the destination does not exist in the network, a RREP packet cannot be generated by any node in the network and all the nodes keep on flooding the RREQ packet. When a large number of fake RREQ packets are broadcast into the network, new routes can no longer be added and the network is unable to transmit data packets. Thus, it leads to congestion in the network and overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a DoS attack. Moreover, unnecessary forwarding of these fake RREQ packets has serious effects in MANET [2] as a result of limited computational and power resources of nodes.

However, the AODV protocol can mitigate against this attack by reducing the maximum number of RREQs that a node allowed to send per second.

B. Selfish Attack on AODV

In MANETs the nodes cooperate to forward data and routing packets from one node to another node. A selfish node is the node that saves its resources; such as battery, by not cooperating in the network operations. A selfish node affects the network performance as it does not correctly process routing or data packets based on the routing protocol. The selfish node behavior is known as a selective existence attack [4]. Selective existence is kind of a passive attack as the node neither participates in the network operation nor changes the content of packets.

The selfish node does not even send any HELLO messages and drops all data and control packets even if these packets are sent to it. When a selfish node needs to send data to another node, it starts working as normal AODV operation. After it finishes sending its data, the node returns to its silent mode and the selfish behavior by dropping all data and routing packets directed through it. Neighbor nodes detect the absence of the selfish node after an interval of silence, and will assume that the node has left their neighborhood. So, they invalidate their own route entries to this node and selfish node becomes invisible to the network.

C. Grayhole Attack on AODV

In a grayhole attack [7], a malicious node behaves normally as a truthful node during the route discovery process by replying with true RREP messages to the nodes that started RREQ messages. After the source node starts sending data through the malicious node, the malicious node starts dropping these data packets to launch a (DoS) denial of service attack. So, the malicious node forwards routing packets and drops data packets. This selective dropping makes grayhole attacks much more difficult to detect than blackhole attacks. Grayhole attack is also known as node misbehaving attack [1] as the malicious node misleads the network by agreeing to forward the packets in the network.

D. Blackhole Attack on AODV

In a blackhole attack [11], a malicious node absorbs the network traffic and drops all packets. To carry out a blackhole attack, a malicious node waits for incoming RREQ packets from other nodes. When the malicious node receives an RREQ message, without checking its routing table, it immediately sends a false RREP with a high sequence number and zero hop count to spoof its neighbours that it has the best route to the destination. Thus, the malicious node reply will be received by the source node before any reply from other nodes. When a source node receives multiple RREP, it chooses the RREP with the largest destination sequence number and the smallest hop count. Then the source node ignores other RREP packets and begins sending data packets over the malicious node. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the destination node.

The malicious node attacks all RREQ packets in this way and takes over all routes. Therefore all packets are sent to a point where they are not forwarding anywhere. If the malicious node generates false RREP messages that appear to come from another victim node, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

III. Attack Simulations

We simulated various attacks on the AODV protocol using the ns-2 simulator [8]. The parameters used are shown in Table I. Node mobility was modelled with the random waypoint method. Each configuration was repeated 12 times. We found that the effect of the pause times used, (0, 10, 20, and 30 seconds) had little effect on the results, so the points representing the results for any particular speed are the mean of the 48 runs, ignoring the pause time. In all cases, the 90% confidence interval was small compared with the values being reported.

While we examined the effects of the attacks on both UDP and TCP traffic, we focused in this paper on their impact on the TCP traffic only. The major difference between TCP and UDP is that the source node keeps on sending UDP packets, even if the malicious node drops them, while it closes the connection after a while if it uses TCP protocol because of not receiving the TCP ACK packet. Although both types of traffic report throughputs, they are not directly comparable, because UDP traffic that is lost is ignored - each packet is treated independently. TCP packets that are lost will be retransmitted by the protocol, and TCP also adapts to the throughput it is achieving using a feedback algorithm. The throughput of UDP can be compared directly with the offered traffic and should match the packet loss rate. In TCP packet loss will have a feedback effect and restrict future transmission rates, but the actual lost packet will be retransmitted. In addition, the data sending rate of UDP can be controlled using simulation which is not valid in TCP. Thus packet loss and throughput for the two protocols are not directly comparable. Furthermore we would like to see the effect of these attacks on sending data which will be evaluated in TCP connection only. The metrics used to evaluate the performance are given below.

TABLE I. SIMULATION PARAMETERS

Simulation Time	180 s
Simulation Area	1000 m x 1000 m
Number of Nodes	100
Number of Connections	70
Number of Malicious Nodes	0 - 5
Node Speed	0 - 30 m/s
Pause Time	0 - 30 s
Traffic Type	CBR - TCP
CBR Rate	4 packets/s

Throughput: This is the number of data bits delivered to the application layer of destination node in unit time measured in bps.
End-to-End Delay: This is the average time taken for a packet to be transmitted across the network from source to destination.
Routing Overhead: This is the number of routing packets for route discovery and route maintenance needed to send to deliver the data packets from sources to destinations.
Route Discovery Latency (RDL): This is the average delay between the sending RREQ from a source and receiving the first corresponding RREP.

A. Flooding Attack on AODV

Fig. 1 shows the effect of malicious nodes on the network throughput when the node mobility is increased. The result shows that the throughput decreases by 10% for each malicious node introduced in the network. This is independent of the node mobility.

The effect of malicious nodes on the end-end-delay when the node mobility is increased is shown in Fig. 2. The result shows that the delay increases as more malicious nodes are added in the network, independent of the node speed.

Fig. 3 shows the effect of malicious nodes on the routing overhead when the node mobility is increased. The result shows that the routing overhead increases 25% in the average as the number of malicious nodes in the network increases.

The effect of malicious nodes on the routing discovery latency when the node mobility is increased is shown in Fig. 4. The result shows that in a static network, the RDL increases 43% for the first malicious node and after that it increases about 27% in the average for each extra malicious node in the network. It is interesting to observe that when the nodes move at all, the malicious nodes have almost no effect on RDL.

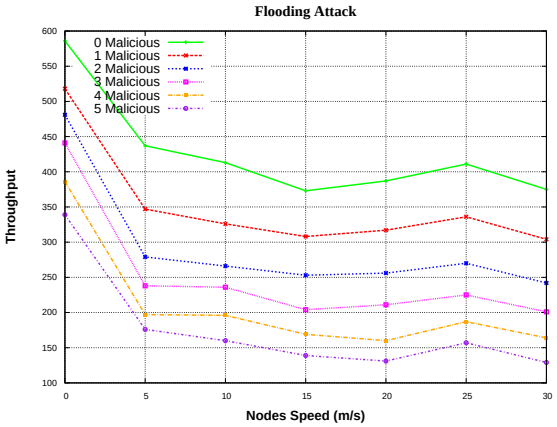

Fig. 1. Throughput under Flooding Attack

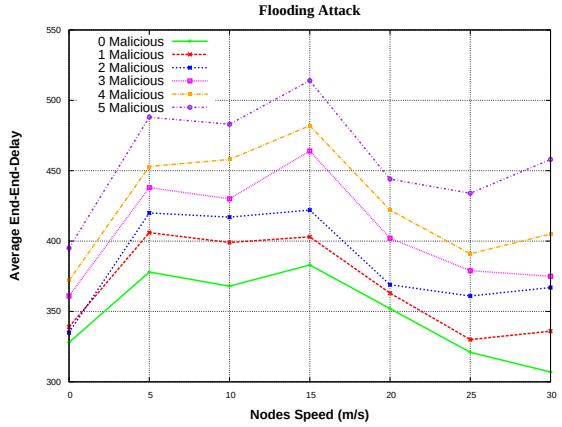

Fig. 2. Average End-End-Delay under Flooding Attack

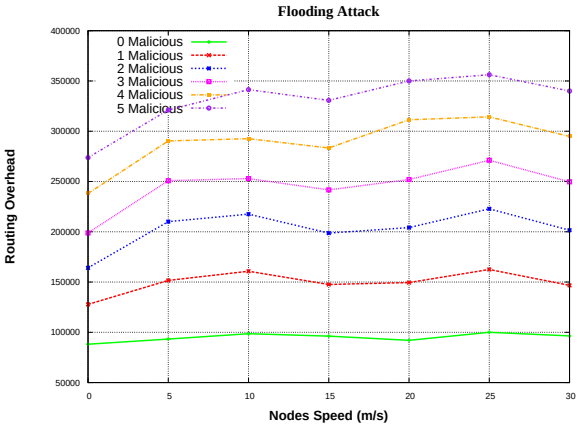

Fig. 3. Routing Overhead under Flooding Attack

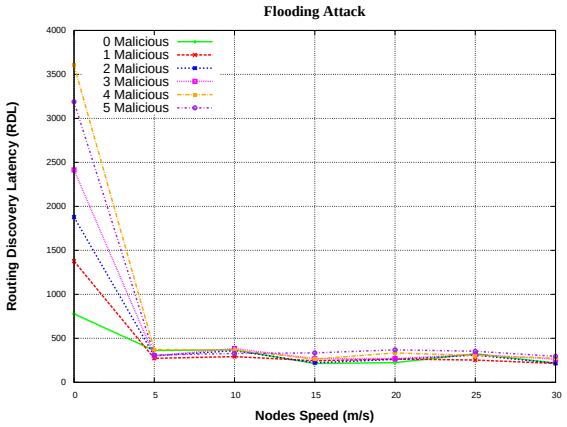

Fig. 4. Routing Discovery Latency under Flooding Attack

B. Selfish Attack on AODV

Fig. 5 shows the effect of malicious nodes on the network throughput when the node mobility is increased. The result shows that the malicious nodes do not have a significant effect on the network throughput.

Fig. 6 shows the effect of malicious nodes on the end-end-delay when the node mobility is increased. The result shows that the delay increases up to 10% in the average as the number of malicious nodes increases for low mobility networks while decreases up to same percentage for the high mobility networks.

The effect of malicious nodes on the routing overhead when the node mobility is increased is shown in Fig. 7. The result shows that the routing overhead decreases up to 6% in the average while increasing the number of malicious nodes in low speed nodes. This percentage rises to 15% in high speed nodes.

Fig. 8 shows the effect of malicious nodes on the routing discovery latency when the node mobility is increased. The result shows that the existence of the first two malicious nodes does not have a major difference in the RDL of routes while the effect becomes remarkable with the existence of any other malicious nodes.The latency in routes discovery increases up to 65% related to the latency time of the AODV without any malicious nodes.

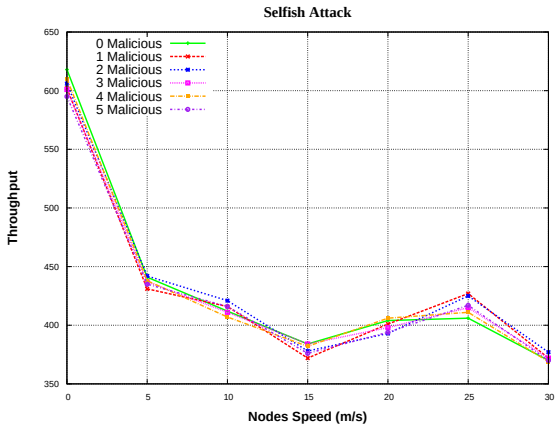

Fig. 5. Throughput under Selfish Attack

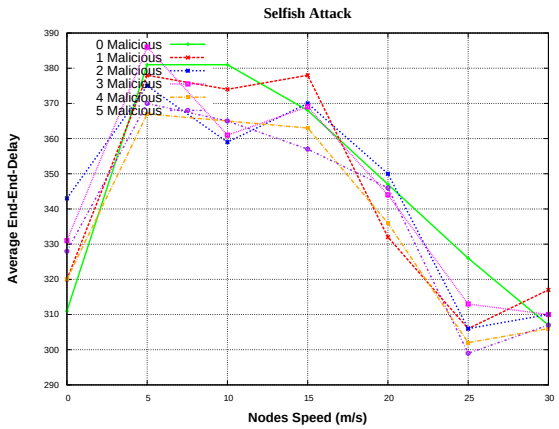

Fig. 6. Average End-End-Delay under Selfish Attack

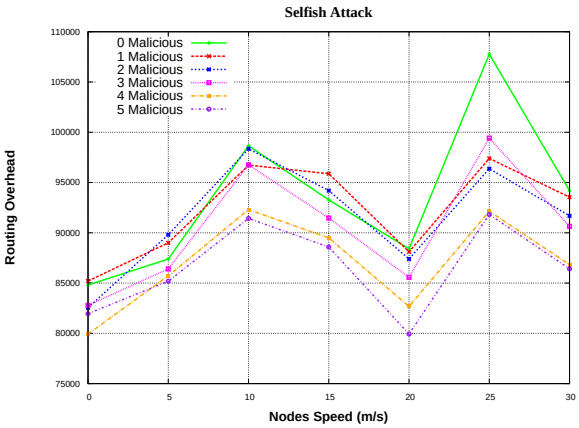

Fig. 7. Routing Overhead under Selfish Attack

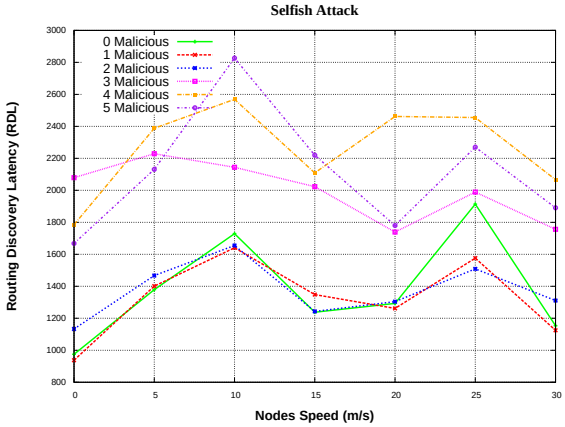

Fig. 8. Routing Discovery Latency under Selfish Attack

C. Grayhole Attack on AODV

As the grayhole node drops all data packets and the selfish node drops all data and routing packets, the grayhole attack simulation introduces very similar results to the selfish attack. This is because of the network throughput, end-end-delay and routing overheads are calculated based on the received data packets which are the unique for the same simulation scenario. The only major difference between simulation results of grayhole attack and selfish attack is in the RDL. Fig. 9 shows the effect of malicious nodes on the routing discovery latency when the node mobility is increased. The result shows that the RDL increases up to 20% for static nodes while decreases up to 40% for high mobility nodes.

D. Blackhole Attack on AODV

Fig. 10 shows the effect of malicious nodes on the network throughput when the node mobility is increased. The result shows that the throughput dramatically decreases 13% with the existence of first malicious node and then the throughput decreases with an average 13% for each malicious node.

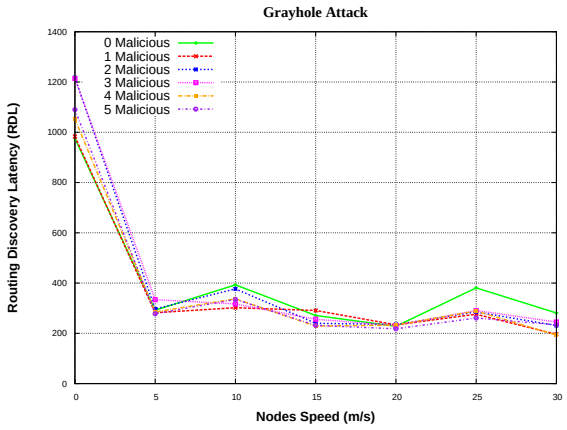

Fig. 9. Routing Discovery Latency under Grayhole Attack

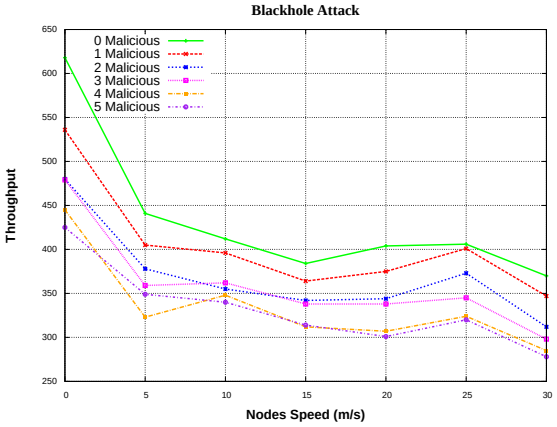

Fig. 10. Throughput under Blackhole Attack

The effect of malicious nodes on the end-end-delay when the node mobility is increased is shown in Fig. 11. The result shows that the delay decreases as the number of malicious nodes in the network increases. This results seems to be unexpected specially if we notice that the same experiment increases the delay for the UDP protocol. The reason of

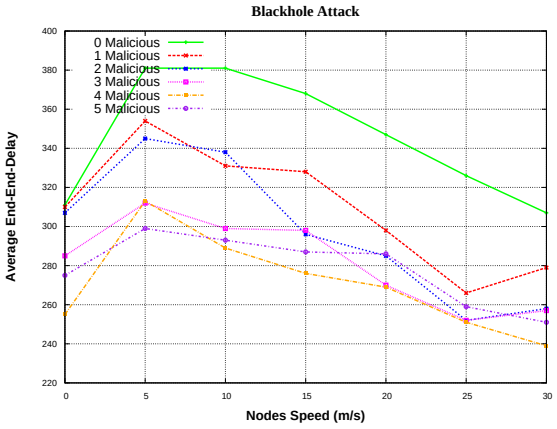

Fig. 11. Average End-End-Delay under Blackhole Attack

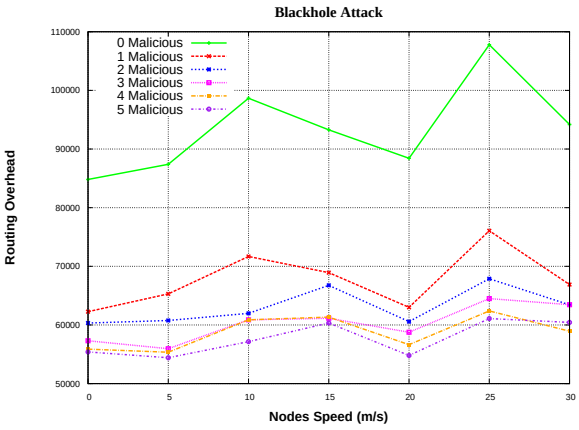

Fig. 12. Routing Overhead under Blackhole Attack

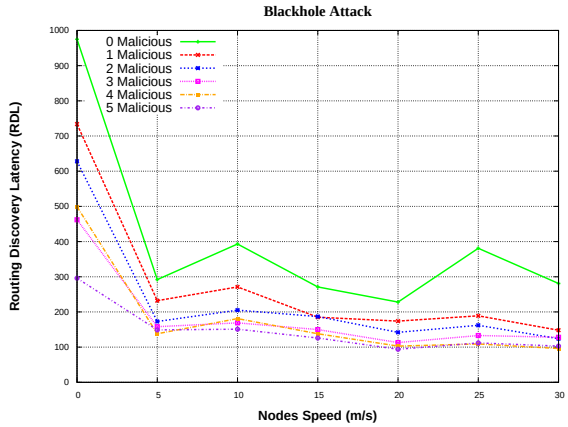

Fig. 13. Routing Discovery Latency under Blackhole Attack

unexpected TCP results may because the existence of the ACK packet which closes the connection if not received within the timeout as specified in TCP. This needs more investigation in future work.

Fig. 12 shows the effect of malicious nodes on the routing overhead when the node mobility is increased. The result shows that the routing overhead increases 27% for the first malicious node while the other malicious nodes have not a large significant effect on routing overhead while increasing the number of malicious nodes in the network.

The effect of malicious nodes on the routing discovery latency when the node mobility is increased is shown in Fig. 13. The result shows that the RDL decreases to approximately 60% in the average while increasing the number of malicious nodes in the network.

The simulation results show as well that the grayhole and selfish attacks have a negative impact on the number of dropped packets. The number of dropped packets relative to the number of malicious nodes for each attack is shown in Fig. 14. The attack type also affects the number of data packets that can be sent during the simulation time. Fig. 15 shows that the blackhole and the flooding attacks affect dramatically the number of data packets sent during the simulation time.

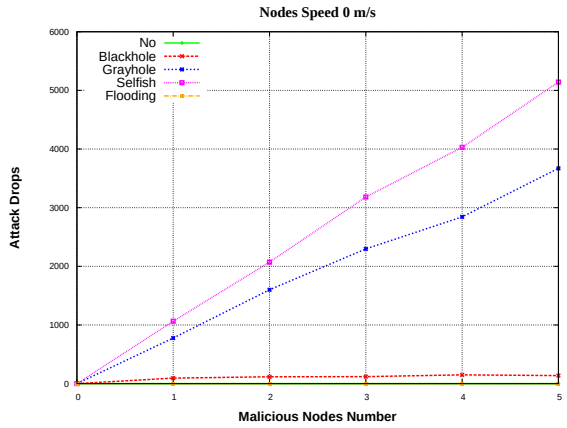

Fig. 14. Number of Dropped Packets by Malicious Nodes

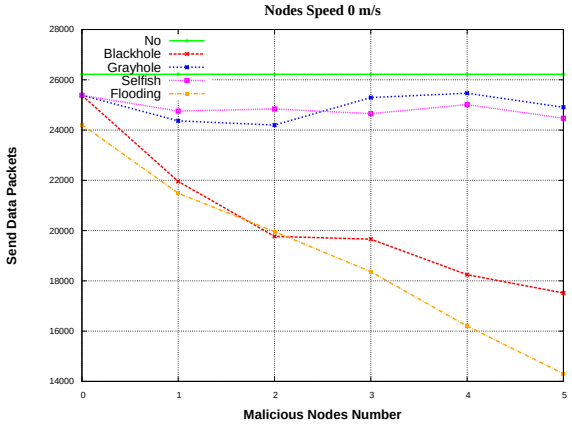

Fig. 15. Number of Sent Data Packets by All Nodes

As we mentioned before, we used both TCP and UDP traffic to evaluate the impact of these attacks on both types of connections. From the simulation we found that the effect of these attacks is very similar in both of these protocols. As an example, Fig. 16 shows the effect of malicious nodes on the network throughput when the node mobility is increased using CBR traffic. We can notice that this figure is close to the Fig. 10 which shows the effect of malicious nodes on the network throughput using TCP traffic.

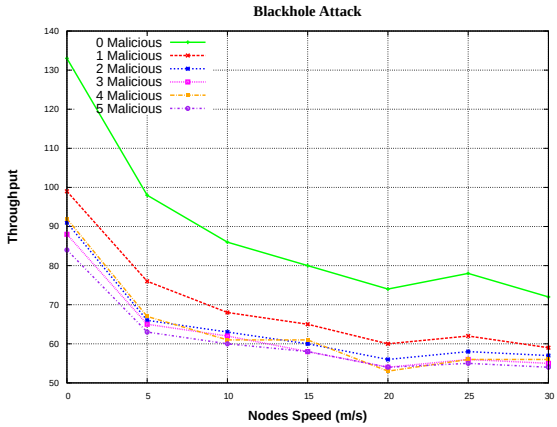

Fig. 16. Throughput under Blackhole Attack using CBR Traffic

IV. Conclusion

In this paper, we analyse the impact of some of the attacks on the AODV routing protocol. The flooding, selfish, grayhole and blackhole attacks are simulated using NS-2 network simulator to study their effects on the performance metrics such as network throughput, end-end-delay, routing overhead and routing discovery latency.

From the simulation, we conclude that the blackhole and flooding attacks have dramatic impact on throughput, end-end-delay and routing overhead. Selfish and grayhole attacks do not affect so much in these metrics because both attacks drop the data packets which are the major factor in calculating these metrics. While selfish and grayhole attack share the data dropping, the blackhole introduce a fake RREP which affects the network performance and the flooding attack introduces a fake RREQ which affects the network performance as well.

References

[1] M. Arya and Y. K. Jain. Grayhole attack and prevention in mobile adhoc network. *International Journal of Computer Applications*, 27(10):21–26, August 2011.

[2] A. Bandyopadhyay, S. Vuppala, and P. Choudhury. A simulation analysis of flooding attack in MANET using ns-3. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1–5, 2011.

[3] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bölöni, and D. Turgut. Routing protocols in ad hoc networks: a survey. *Computer Networks*, 55(13):3032–3080, September 2011.

[4] P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications*, 9(12):11–15, November 2010.

[5] Y. Guo and S. Perreau. Detect DDoS flooding attacks in mobile ad hoc networks. *Int. J. Secur. Netw.*, 5(4):259–269, Dec. 2010.

[6] A. Kumar. Security attacks in MANET - a review. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[7] K. Manikandan, R.Satyaprasad, and K.Rajasekhararao. A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks. *IJACSA - International Journal of Advanced Computer Science and Applications*, 2(3):7–12, 2011.

[8] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[9] M. Patel and S. Sharma. Detection of malicious attack in manet a behavioral approach. In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, pages 388–393, 2013.

[10] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1997.

[11] N. Sharma and A. Sharma. The black-hole node attack in MANET. In *Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies*, ACCT '12, pages 546–550, Washington, DC, USA, 2012. IEEE Computer Society.

[12] M. Singh, A. Singh, R. Tanwar, and R. Chauhan. Security attacks in mobile adhoc networks. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[13] G. Usha and S. Bose. Impact of gray hole attack on adhoc networks. In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pages 404–409, 2013.