A Performance Study of Various Security Attacks on AODV Routing Protocol in MANET

Kuldeep Singh
Student, B.E. (final year), CSE
UIET, Panjab University,
Chandigarh, India

Sudesh Rani
Assistant Professor, CSE
Punjab Engineering College,
Chandigarh, India

ABSTRACT

Mobile Ad-hoc Network (MANET) is a self-configuring wireless network of movable and independent nodes which operate without the support of any permanent infrastructure, hence MANET has dynamic topology. In MANET, each node forwards traffic unrelated to its own use. Despite the proliferation of MANET, it is prone to various attacks which include blackhole attack, grayhole attack, flooding attack, wormhole attack etc.

This paper presents the analysis of the effect of various security attacks on the performance of AODV routing protocol against various parameters such as throughput, packet delivery ratio, packet loss, and mean-hop, normalized routing overhead and end-to-end delay.

Keywords

AODV, MANET, Blackhole Attack, Flooding Attack, Grayhole Attack, Attacker node, Selfish node

1. INTRODUCTION

MANET (Mobile Ad-hoc Networks) is a self-configuring and infrastructure-less network of mobile devices in which nodes can move freely and independently and are connected via wireless links. Each node in these networks also works as router to forward traffic not related to its own use. Ad hoc environments are attractive for military applications and disaster response situations where fixed networking infrastructures may not be available once damaged beyond use. MANET [1] can be implemented using various routing protocol like AODV, DSR, DSDV etc. In this paper AODV (Ad-hoc On-demand Distance Vector) routing protocol [2] is used because it is an on-demand routing protocol and has better security as compared to other protocols. It uses route request (RREQ) and route reply (RREP) packets to create a connection between source and destination.

MANET is vulnerable to various types of attacks which are categorized as active and passive attacks [3]. Active attacks include attacks which interfere with the normal functioning of the network. Blackhole attack, Grayhole attack, Warmhole attack and flooding are some examples of active attacks [4] in MANET. In Blackhole attack, an attacker node is present which attract the network traffic by providing false information about optimal path to destination. Grayhole attack differs from black hole attack in the sense that it can have any node as attacker at any random instance of time in network and hence makes it difficult to detect. Wormhole attack consists of two attacker nodes which attracts traffic and transfers traffic to other node via a high speed link called as tunnel. Flooding attack [5] is another type of active attack which continuously floods the network with RREQ/data packets. This attack disrupts the normal functioning of network by un-necessarily using bandwidth and increasing routing overhead by considerable amount and sometimes leads to network crash.

This paper is organized as follows. Section-II describes AODV[6] routing protocol and various attacks which are considered in this paper for performance evaluation of AODV in MANET such as black hole [7] attack, grayhole attack and flooding attack. Section-III gives the details of the simulation environmental used in NS Simulator. Section-IV presents the analysis of the results based on throughput, packet delivery ratio, mean hop, packet loss, normalized routing overhead, and end-to-end delay. Section V presents the final conclusion.

2. BACKGROUND

In this paper, AODV protocol is used to implement blackhole and grayhole attacks in MANET. It is an on demand routing protocol which establishes route between source and destination only when a source needs to send some data to destination. AODV uses route request RREQ and route reply RREP to setup the desired route. When a source desires a route then it broadcasts a route request RREQ packet across the network. Sequence number is used to determine the fresh route to the destination. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

MANET is vulnerable to various types of attacks which are categorized as active and passive attacks. Passive attacks are hard to detect because these attacks don’t interfere with the normal working of the network. These attacks target the confidentiality of the system. This type of attacks includes eavesdropping, traffic analysis, monitoring etc. whereas active attacks can be easily detected as compared to passive attacks because these attacks disrupts the normal functioning of the network. This type of attack includes blackhole, grayhole, wormhole, flooding etc.

In the given figures, Red colored nodes represents Attacker or malicious node, Green colored nodes represents source node generating source packets and blue colored nodes are destination nodes for source packets.

2.1 Blackhole Attack

Blackhole is the malicious node in the network (labelled as attacker in Figure 1) which falsely replies to route requests (RREQ) without having an active route to destination and exploits the routing protocol to advertise itself as having a shortest route to the destination. Due to this false information, source starts sending the data to the malicious node which discards the packet and sends a reply (RREP) to source to acknowledge the data packet. Sequence number is used to determine the fresh route from source to destination, route with the highest sequence number is selected for further data transmission. Hence to provide false information to sender, malicious nodes keeps the sequence number high enough so that source only selects the path provided by malicious node. This attack degrades the performance and efficiency of network by greatly decreasing the number of packets successfully delivered to destination and leads to loss of information caused by malicious node.

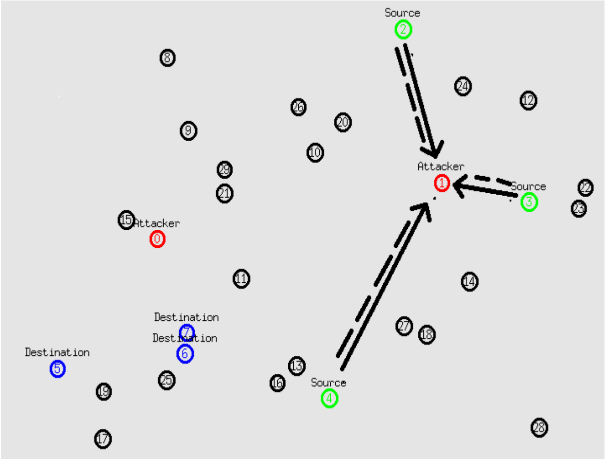

Figure 1: Blackhole Attack with malicious nodes

2.2 Grayhole Attack

Grayhole node in this attack is similar to the malicious node in blackhole attack. Grayhole attack works in two phases. In first phase, grayhole node falsely advertise itself as having a valid and shortest route to the destination with the intention of intercepting packets and dropping them selectively. In second phase, grayhole node drops the packet either deterministically or stochastically for random amount of time. Malicious node in this attack either drops packet coming from specific node or in other case, it drops the data packets for certain random amount of time and behaves normally after that. Grayhole attack (as shown in Figure 2) is hard to detect because malicious node behaves maliciously for random amount of time then behaves as other normal nodes, hence, malicious node in this case is anonymous unlike in blackhole where malicious node drops data packets with certainty.

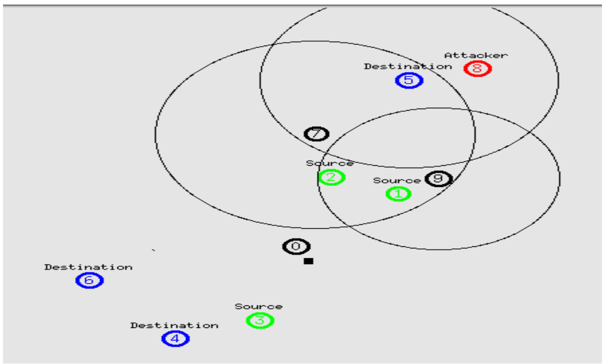

Figure 2: Grayhole Attack with malicious node

2.3 Flooding Attack

Flooding attack is a type of denial of service attack in which a malicious node flood the network with route request (RREQ) packets having destination node numbers not present in the current network topology (as shown in Figure 3). Malicious node flood two types of packets either data packets or route request packets and continuously sends these packets without waiting for reply from other nodes. Malicious node makes other nodes busy in forwarding requests to other nodes and hence, it affects the overall throughput and packet delivery ratio of network. It also greatly affects the performance of the network by consuming bandwidth un-necessarily and increases the routing overhead exponentially in the network. It may sometimes lead to network crash because of unmanageable number of routing/data packets.

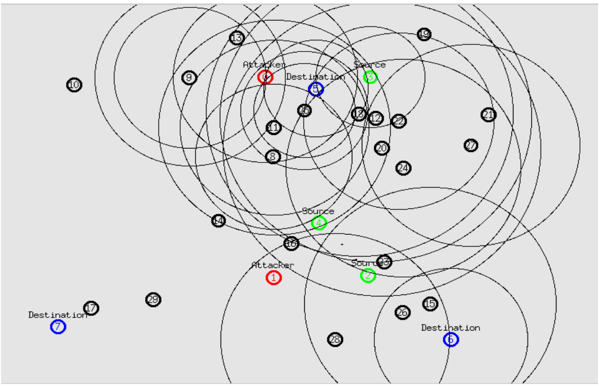

Figure 3: Flooding Attack with malicious nodes

3. EXPERIMENTAL SETUP

The performance of AODV routing protocol in MANET is analyzed against parameters such as Packet delivery ratio, mean hop count, packet loss, average throughput in kbps, normalized routing overhead, end-to-end delay under various scenarios using NS-2.35 simulator. Three source and three destinations are used along with zero/one./two attacker nodes. In grayhole attack, attacker node is selected and activated at random time from the available nodes. In flooding attack, attacker node floods the packet in network at a time interval of 90ms. In blackhole attack, predefined nodes act as attackers throughout the simulation. Simulations are run on 10 seeds and average of the obtained parameter values are used for final analysis and comparison. To analyze the performance of AODV protocol, scenarios are set as per the parameters shown in table below.

Table 1: Experimental Setup

Simulation Time	500.0 sec
Topology	Mobile
Node Placement	Random
Terrain Dimension	800 x 550
Antenna Model	OmniAntenna
Number of Nodes	10, 20, 30, 40
MAC Layer	802.11
Routing Protocol	AODV
Radio Propagation Model	TwoRayGround
Traffic Model	Constant Bit Rate
Packet Size	256
Traffic Rate	0.1 mbps

4. PERFORMANCE METRICS

AODV routing Protocol is used for simulation in various network densities and node distribution. It is assumed that link between nodes is bidirectional and circular. The performance can be measured by variety of metrics:

4.1 Throughput

Throughput is rate of packets delivered successfully to destination per unit time.

∑ No. of packets received / (Stop Time – Start Time)

High the throughput corresponds to the better performance of the protocol.

4.2 Packet Delivery Ratio (PDR)

Packet Delivery Ratio is the ratio of number of packets delivered to the destination to the number of packets sent. This illustrates the quantitative analysis of packets delivered to destination successfully.

∑ Number of packets received / ∑ Number of packets sent

High value of PDR corresponds to the better performance of the protocol.

4.3 Normalized Routing Overhead

Normalized Routing Load is the ratio of number of routing packets to the number of data packets delivered to the destination.

∑ No. of Routing packets / ∑ No. of data packets

Low normalized routing overhead corresponds to the better performance of the protocol.

4.4 End to End Delay

It is the average time taken by a data packet to arrive at destination from the source. It includes the delay caused by routing process and the queue in data transmission process. Only the data packets that are successfully delivered to destination are counted.

(Arrive time – send time) / ∑ Number of connections

Low value of End-to-end delay corresponds to the better performance of the protocol.

4.5 Packet Loss

Packet loss is the number of packets dropped or lost per unit time during simulation.

$$\frac{(\sum \text{No. of packets sent} - \sum \text{No. of packets received})}{(\text{Stop Time} - \text{Start Time})}$$

Low value of packet loss corresponds to the better performance of the protocol.

4.6 Mean Hop count

Mean hop is the ratio of number of packets forwarded to the number of packets sent.

∑ No. of packets forwarded / ∑ No. of packets sent

Low mean hop count better corresponds to the better performance of the protocol.

5. RESULTS

We have compared the throughput, mean hop, packet delivery ratio, packet lost, normalized routing overhead, end-to-end delay of the Mobile Ad-hoc network for AODV routing protocol without any attack and AODV routing protocol in the presence of blackhole, grayhole and flooding attack. In the results, following abbreviations are used:

ADOV: AODV without any attack.

BHAODV1: AODV with one blackhole attacker node.

BHAODV2: AODV with two blackhole attacker nodes.

GHAODV1: AODV with one grayhole attacker node.

GHAODV2: AODV with two grayhole attacker nodes.

FAAODV1: AODV with one malicious node.

FAAODV2: AODV with two malicious nodes.

5.1 Throughput vs Number of nodes

The effect on the network throughput with respect to no. of nodes is shown in figure 4. It can be seen from the graph that in presence of blackhole attack, the throughput of network drops significantly. On the other hand, the effect on throughput due to grayhole attack is less as compared to blackhole for same number of attacker nodes. Flooding attack has least effect on throughput among the three attacks. Also, if more than one malicious node is present in the network, throughput further decreases in case of each security attack.

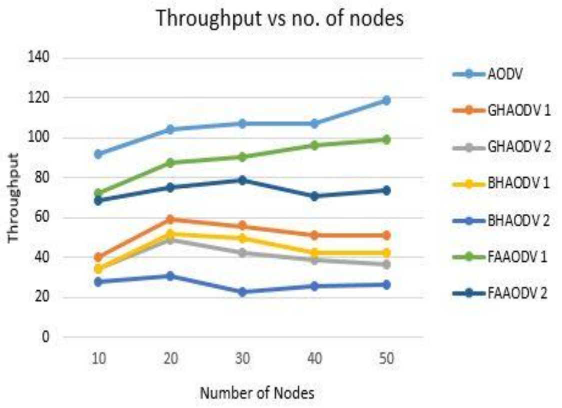

Figure 4: Throughput vs Number of Nodes

5.2 Packet Delivery Ratio vs No. of Nodes

Figure 5 shows the effect on Packet delivery ratio with respect to no. of nodes. From the graph, it can be seen that in presence of blackhole attack, the packet delivery ratio of network drops significantly. On the other hand, the effect on packet delivery ratio due to grayhole attack is less as compared to blackhole for same number of malicious node. Flooding attack has least effect on packet delivery ratio among the three attacks. Also, if more than one malicious node is present in the network, packet delivery ratio further decreases in case of each security attack.

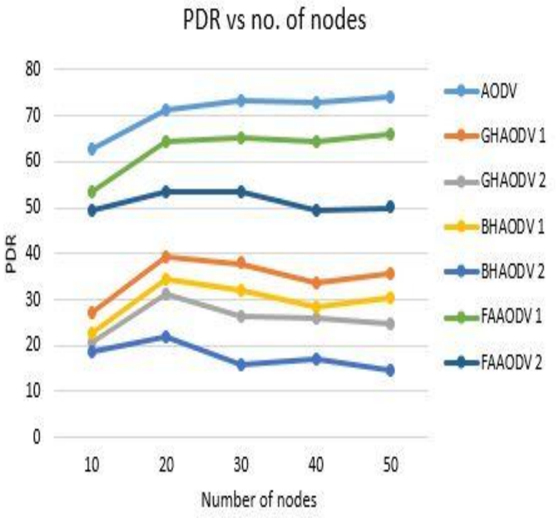

Figure 5: Packet Delivery Ratio vs Number of Nodes

5.3 Normalized Routing Overhead vs Number of Nodes

Effect of malicious node on AODV protocol in terms of normalized routing overhead with respect to no. of nodes is shown in figure 6. It is clear from the graph that flooding attack has most significant effect on the network as compared to other attacks. As the number of nodes increases, the effect of blackhole and grayhole attack does not increase significantly but in case of flooding, effect of malicious node increases almost exponentially, hence can lead to network failure. It can be seen from results that flooding attack has most significant effect on routing overhead only and very less impact on other parameters.

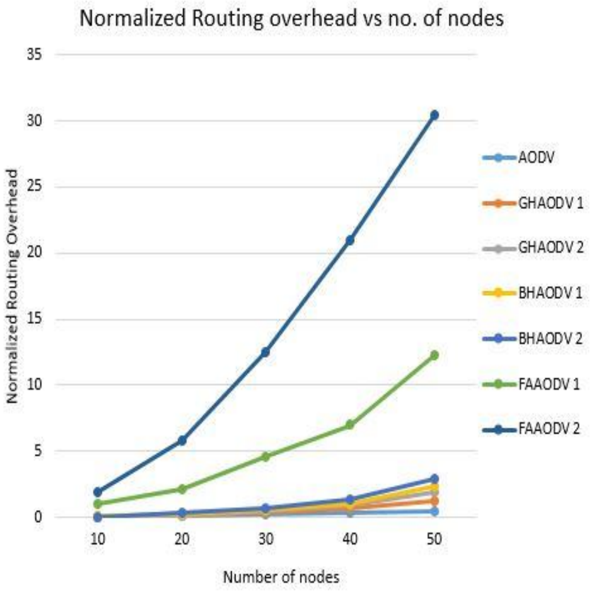

Figure 6: N. Routing Overhead vs No. of Nodes

5.4 End to End delay vs Number of Nodes

The effect of malicious nodes on end to end delay is depicted in figure 7. To analyze end to end delay, only one malicious node is considered for all the attacks. It can be seen from the results that blackhole node has the most significant effect on end to end delay followed by grayhole and then by flooding attack. It is because of the fact that blackhole node is active all the time whereas grayhole node was active for random period of time.

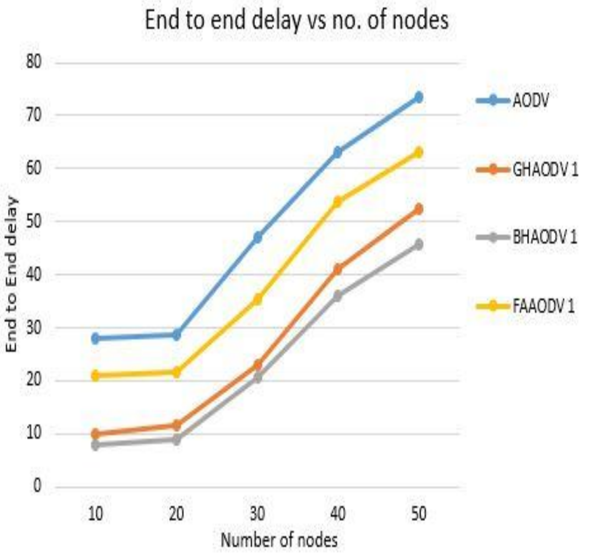

Figure 7: End to End Delay vs Number of Nodes

5.5 Packet Loss vs Number of Nodes

Figure 8 shows the number of packets dropped during simulation either because of malicious node or because of wireless nature of the network. It is clear from the graph that blackhole attack is most severe effect on network followed by grayhole and then flooding attack. It is because the blackhole node is active all the time where as grahole node is active only for random amount of time which is less than the blackhole node's active time. As the number of malicious nodes increases, the effect of these nodes further increases.

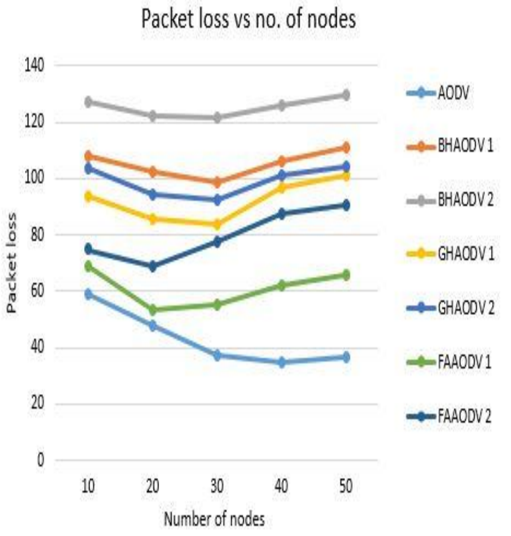

Figure 8: Packet loss vs Number of Nodes

5.6 Mean hop vs Number of Nodes

In figure 9, effect of malicious nodes on mean hop count is analyzed. It can be analyzed from the graph that the effect of malicious nodes does not vary significantly. Meanhop count is decreased greatly due to blackhole attack followed by grahole and the flooding attack.

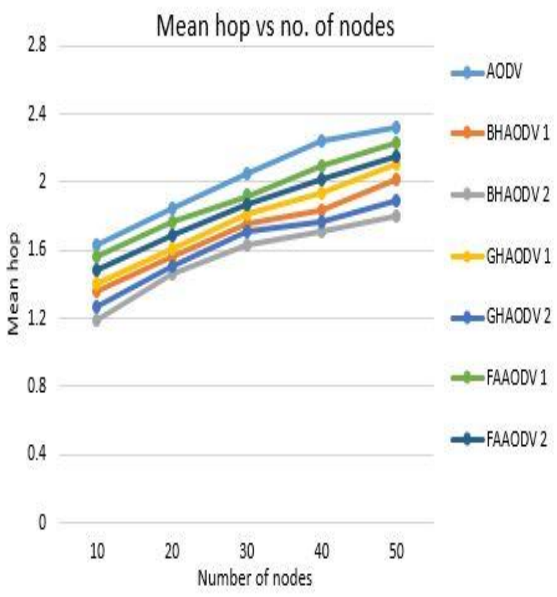

Figure 9: Mean hop vs Number of Nodes

6. CONCLUSION AND FUTURE WORK

This paper presents the analysis and effect of blackhole, grayhole and flooding attack on the performance of AODV routing protocol in MANET. These attacks add to the limitations caused by the dynamic nature of nodes in MANET. From the results, it can be concluded that flooding attack increases the routing overhead exponentially and can even lead to the crash of whole network. However, flooding attack has lesser impact against other parameters except normalized routing overhead. On the other hand, blackhole has more severe impact than grayhole because of the malicious node, which is active throughout the simulation. But in grayhole attack, malicious node can be any random node, and activated at random time. This causes the malicious node in case of grayhole attack act as malicious node only for some random time which is always less than the total active time of malicious node in case of blackhole attack.

From the results it can be concluded that blackhole attack is the most severe attack for AODV routing protocol among all other attacks in respect of various performance measures. But severity of attack also depends whether the attack is detectable or not. It can be further analyzed that the attacker node in case of blackhole attack is a fixed node which is active throughout the simulation, whereas the attacker node in case of grayhole attack is any random node which is active and remain active for random amount of time. Hence, it is easy to detect a blackhole node because it is fixed and active all the time. On the other hand, grayhole node is difficult to detect because of its dynamic nature. This leads to the conclusion that grayhole attacker node, being anonymous, can have more impact than blackhole attacker node if detection and removal of attacker is also implemented.

In future, the analysis can be expanded by adding more security attacks using AODV routing protocol and by adding comprehensive analysis of the effect of various security attacks on both AODV and DSR routing protocol.

7. REFERENCES

[1] Andel, Todd R., and Alec Yasinsac. "Surveying security analysis techniques in MANET routing protocols." Communications Surveys & Tutorials, IEEE 9.4 (2007): 70-84.

[2] Perkins, Charles E., and Elizabeth M. Royer. "Ad-hoc on-demand distance vector routing." Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999.

[3] Liang, Yingbin, H. Vincent Poor, and Lei Ying. "Secrecy throughput of MANETs under passive and active attacks." Information Theory, IEEE Transactions on 57.10 (2011): 6692-6702.

[4] Konate, Karim, and G. A. Y. E. Abdourahime. "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation." Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on. IEEE, 2011.

[5] Bandyopadhyay, Alokparna, Satyanarayana Vuppala, and Prasenjit Choudhury. "A simulation analysis of flooding attack in MANET using NS-3." Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

[6] Dembla, Deepak, and Dr Yogesh Chaba. "Modeling and Analysis of an intelligent AODV Routing Protocol based on Route Request Retransmission Strategy in MANETs." International Journal of Computer Applications (0975-8887) Volume (2011): 6-13.

[7] Ruiz, Juan-Carlos, et al. "Black Hole Attack Injection in Ad hoc Networks." Fault tolerance systems group (GSTF). http://www. ece. cmu. edu/~ koopman/dsn08/fastabs/dsn08fastabs_ruiz. pdf (2011).