International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

Detection of Black Hole Attacks in AODV routing protocol in MANET

Ms. Varsha Rajesh Shinde[1], Prof. Mr. Y. R. Kalshetty[2]

[1]PG student CSE Dept., SVERIs college of Engineering, Pandharpur, Maharashtra, India
[2]Assistant Professor CSE Dept., SVERIs college of Engineering, Pandharpur Maharashtra, India

---

Abstract - *MANETs are open and co-operative networks and can be formed quickly as well as without any complicated infrastructure. These are very useful characteristics for fast and easy connectivity; but this poses severe security threats. In this paper, we only focus on the review of detection of black hole attacks in AODV routing protocol. Black Hole attack is also called sequence number attack because it is created using and modifying sequence number field in routing control packets. We have reviewed the attack and its detection method on a of the well known and largely used MANET routing protocol known as Ad Hoc Distance Vector (AODV) routing protocol. The performance is analyzed based on throughput, message delay and routing overhead, etc.*

Key Words: Black Hole Attack, AODV, NS-3, MANET

1. INTRODUCTION

Security and privacy are main aspects of any type of communication. MANET has many advantages over the wired network that makes it highly useful in many fields where wired network cannot be operated. The network performance is lower if a malicious node is present in the given network. A malicious node can exploit the vulnerabilities in the MANET in different ways. Routing protocol in MANET is another important part that plays very important role in data delivery. A node can violate the routing rules causing damage to data transmission.

Routing protocol can lead to different malicious behaviors, like modifying routes, dropping a packet, forging of routing control messages. That's why intruder targets the routing protocols to attack MANET. By attacking routing protocol, alone MANET can be attacked in many ways; like Hello Flooding Attack, wormhole attack, Location-Disclosure, Rushing Attacks, Invisible Node, and Routing Table Attack. Black Hole attack is another attack that disrupts networks data traffic flow. Hence a mobile ad hoc network needs a secure routing protocol to have reliable data flow from source to destination.

MANET has proved very useful over traditional networks in difficult conditions. In MANET all mobile devices work cooperatively for route discovery as well as data transmission. Due to its broadcast nature of transmission, and cooperative model of working, routing the traffic is a tiresome task in MANET. Routing protocols are constantly targeted by attackers to cause harmful effects to network. MANET needs to be robust against various security threats in routing protocols. Ad hoc on-demand distance vector routing (AODV) protocol is widely used also studied in the area of mobile ad hoc networks.

2. METHODOLOGY

2.1 Routing Protocol

Communication between nodes in Ad Hoc networks handled by routing protocols. They maintain information that helps nodes to find routes to required destinations. Routing algorithms set up the path, as well as routes the packets on that path from source to destination. Hence, the effectiveness of communication depends upon the efficiency of the routing algorithm. Various routing algorithms are available in theory. According to the mode of operation, these protocols are classified in two broad categories.

1. Proactive Routing Protocols
2. Reactive Routing Protocols

1. Proactive Routing Protocol: A Routing Table data structure is maintained at every node. In that table all remaining nodes existing paths stored. The table is updated with latest information. Any change in the network topology is reflected in the routing table in no time. So, a node has route information to every other node in all time.

2. Reactive Routing Protocol: In contrast to proactive routing protocols, here the path is setup from source to destination, only when it is needed. The path is maintained up to the data is transmitted. Here two cases are happens; one is source node asks to terminate the path, and second is the path information is deleted after a time limit expires.

Ad hoc On-Demand Distance Vector (AODV)

AODV is a distance vector routing protocol that is included in the classification of the reactive routing protocol, which is just to request a service when needed. This routing protocol determine the route to destination if there is node that wants to transmit data using route request (RREQ) packet that sent by source. If there is active route to the destination, receiver will reply the messages with route reply (RREP) packet. AODV is flat routing protocol it means AODV does not require central administrative system in routing process. Working of AODV is shown in fig 1.

The advantage in AODV routing is providing the change in link situation very easily, but at the same time it can undergo the large delays during route manipulation and consume more bandwidth as the network size increases.

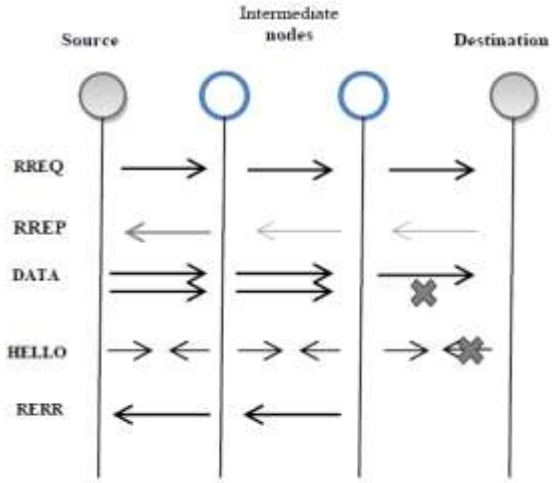


Fig -1: working of AODV

2.2 Security issues

AODV has very limited capability to prevent against security issues. An attacker can exploit several vulnerabilities of AODV, such as absorbing routing packets, modifying and forwarding, false reply or sending false route request messages. In this paper, we are limited to only one type of attack black hole attack. We will present a comparison on the impact of these attack on the AODV based MANETs.

Black Hole Attack

The aim of a black hole attack is to spuriously reply to any RREQs without having an active route to the precise destination, and to drop all the received packets. Black ole attack working is shown in fig 2. An attacker generates a Black hole attack and is able to modify the network topology by creating an auspicious "environment" for the attack. This is accomplished by forging RREQ messages and advertising itself as having the shortest path for the packet to be delivered to the destination, in order to intercept the packets between two authentic nodes. Figure shows how the black hole attack works. In the beginning, the originator node sends RREQs to the network to discover valid routes. A malicious node intercepts a RREQ, sent by the source node; this node then forwards it to the destination node and sends a RREP back to the source node to register itself as a legitimate route.

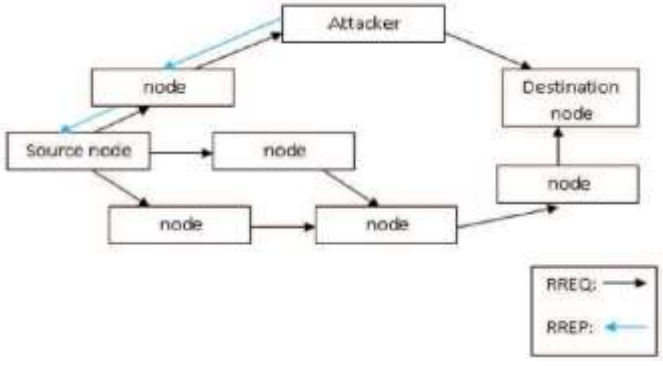


Fig – 2: black hole attack

After that, the source node transfers the data packets as an authentic user within the MANET. Then this malicious node intercepts the data flow by receiving the information but without forwarding it to the destination node. Obviously, the neighbor nodes are able to detect the sequence of the falsified RREQ or RREP messages sent by the malicious node, and then they put the malicious node in their blacklists by terminating the data flow over it. It has been observed that by minimizing the exposure risk, the malicious node/s cannot intercept the data transfer between two related nodes, but still able to transmit the packet/s. Furthermore, the attacker can adequately amend some messages sent from particular nodes, though not from all.

2.3 Black Hole Attack in AODV

AODV is dangerously affected by well-known attack i.e., black hole attack in which a malicious node injects a fake route reply message that it has a fresh route towards destination. An example of black hole attack in AODV is shown in fig 3.

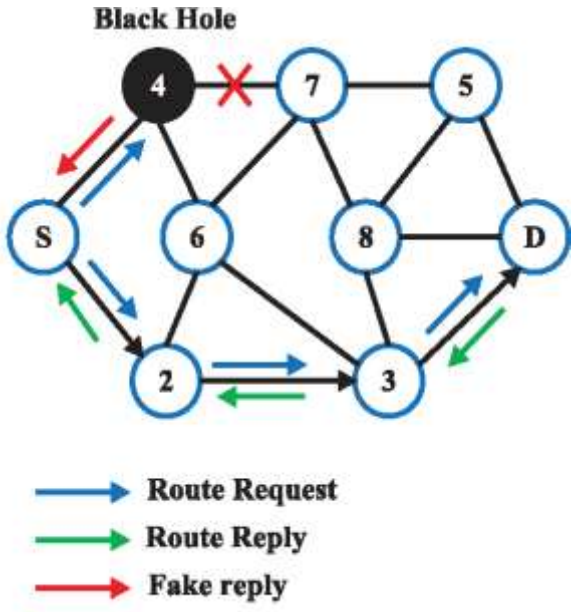


Fig – 3: An example of black hole attack in AODV

There are two phases of this attack which take place sequence, in first phase malicious node detects routing algorithm such as AODV and participate by showing that it is intermediate node and can be trusted because it is nearest to destination. In second phase it shows fake establishment of route by minimum hop count and high sequence number. As a result it starts receiving packets from the source and drops these packets without forwarding them.

3. RESULT AND ANALYSIS

3.1 Existing model

Table 3.1 shows the existing model.

Parameters	Values
Area size	1000m x 1000m
MAC	IEEE 802.11b
Wireless Interface Mode	Ad-Hoc
Propagation Loss Model	Two Ray Ground Propagation Loss Model
Propagation Delay Model	Constant Speed Propagation Delay Model
Number of Nodes	4
Mobility Model	Constant Position Mobility Model
Number of Flows	1
Routing Protocol with Hello Interval	AODV(2s)
Physical Mode	DsssRate1Mbps

Table 3.1: Existing model parameters.

3.2Proposed model

Table 3.2 shows the proposed model of congestion control with hello interval in routing algorithm.

Parameters	Values
Area size	1000m x 1000m
MAC	IEEE 802.11b
Wireless Interface Mode	Ad-Hoc
Propagation Loss Model	Two Ray Ground Propagation Loss Model
Propagation Delay Model	Constant Speed Propagation Delay Model
Number of Nodes	12
Mobility Model	Constant Position Mobility Model
Number of Flows	1
Routing Protocol	AODV, AODV with black hole attack
Hello Interval	0.5s, 1.0s, 1.5s, 2.0s, 2.5s, 3.0s, 3.5s
Packet size	1040
Number of Packets	5
Physical Mode	DSSS 1mbps, 2mbps, 5.5mbps, 11mbps

Table 3.2: Proposed model parameters.

3.3 Throughput

Throughput=(rxBytes/timeLastRxPacket-
timeFirstTxPacket) *(8/1024)kbps

Table 3.3 to 3.6 shows result of throughput.

Hello interval	AODV	AODV with blackhole
0.5	215.078	15.7688
1.0	0	159.67
1.5	156.98	223.321
2.0	15.5476	109.314
2.5	15.8196	15.4183
3.0	226.825	124.078
3.5	15.7095	15.5958

Table 3.3 Results of Throughput at DSSS rate 1mbps.

Hello interval	AODV	AODV with blackhole
0.5	282.505	16.053
1.0	282.505	0
1.5	282.505	8.03205
2.0	282.505	0
2.5	282.505	256.187
3.0	282.505	172.827
3.5	282.505	15.7391

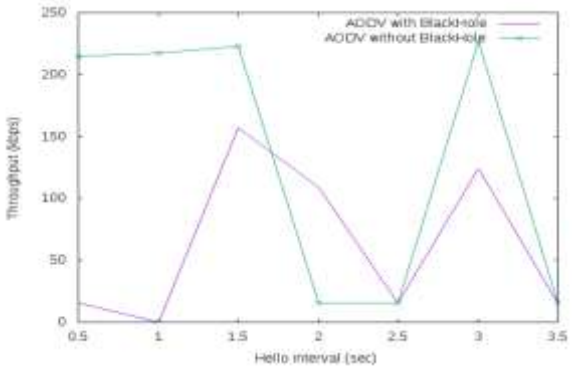
Table 3.4 Results of Throughput at DSSS rate 2mbps.

Hello interval	AODV	AODV with blackhole
0.5	299.608	223.384
1.0	299.608	172.732
1.5	299.608	243.535
2.0	299.608	243.535
2.5	299.608	299.608
3.0	299.608	299.608
3.5	299.608	264.876

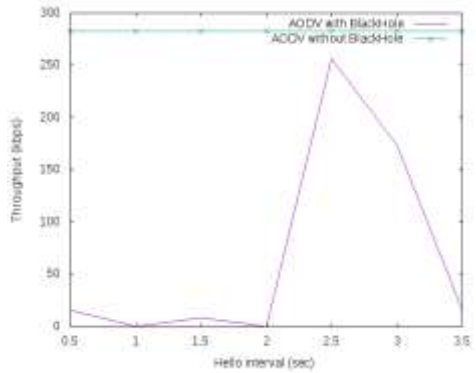
Table 3.5 Results of Throughput at DSSS rate 5.5mbps.

Hello interval	AODV	AODV with blackhole
0.5	304.883	356.188
1.0	304.883	0
1.5	16.4609	0
2.0	304.883	0
2.5	304.883	316.371
3.0	304.883	0
3.5	304.883	0

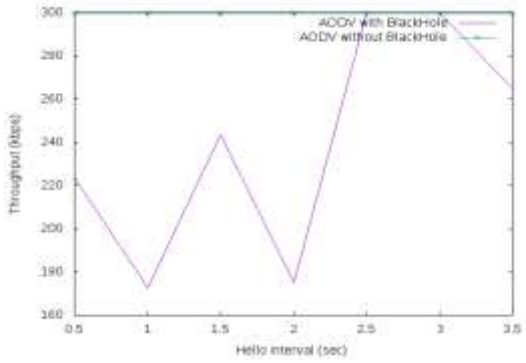
Table 3.6 Results of Throughput at DSSS rate 11mbps.



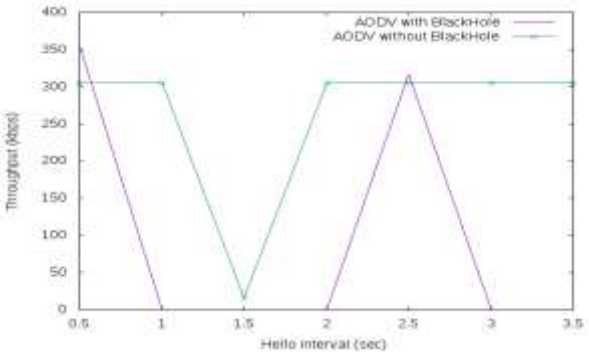
Graph 3.1: Throughput at DSSS rate 1mbps



Graph 3.2: Throughput at DSSS rate 2mbps



Graph 3.3: Throughput at DSSS rate 5.5mbps



Graph 3.4: Throughput at DSSS rate 11mbps

3.4 PDR

PDR =rxBytes/txBytes
Table 3.7 to 3.10 shows result of PDR.

Hello interval	AODV	AODV with blackhole
0.5	1	0.4
1.0	1	0
1.5	1	0.4
2.0	0.4	0.4
2.5	0.4	0.4
3.0	1	0.4
3.5	0.4	0.4

Table 3.7 Results of PDR at DSSS rate 1mbps.

Hello interval	AODV	AODV with blackhole
0.5	1	0.4
1.0	1	0
1.5	1	0.2
2.0	1	0
2.5	1	0.4
3.0	1	0.4
3.5	1	0.4

Table 3.8 Results of PDR at DSSS rate 2mbps.

Hello interval	AODV	AODV with blackhole
0.5	1	0.4
1.0	1	0.4
1.5	1	0.4
2.0	1	0.4
2.5	1	1
3.0	1	1
3.5	1	0.6

Table 3.9 Results of PDR at DSSS rate 5.5mbps.

Hello interval	AODV	AODV with blackhole
0.5	1	0.6
1.0	1	0
1.5	0.4	0
2.0	1	0
2.5	1	0.6
3.0	1	0
3.5	1	0

Table 3.10 Results of PDR at DSSS rate 11mbps.

3.5 Packet Loss Ratio

PacketLossRatio = lostPackets/(rxPackets+lostPackets)
Table 3.11 to 3.14 shows result of packet loss ratio.

Hello interval	AODV	AODV with blackhole
0.5	1	0.6
1.0	1	1
1.5	1	0.6
2.0	0.4	0.6
2.5	0.4	0.6
3.0	1	0.6
3.5	0.4	0.6

Table 3.11 Results of packet loss ratio at DSSS rate 1mbps.

Hello interval	AODV	AODV with blackhole
0.5	0	0.6
1.0	0	1
1.5	0	0.8
2.0	0	1
2.5	0	0.6
3.0	0	0.6
3.5	0	0.6

Table 3.12 Results of packet loss ratio at DSSS rate 2mbps.

Hello interval	AODV	AODV with blackhole
0.5	0	0.6
1.0	0	0.6
1.5	0	0.6
2.0	0	0.6
2.5	0	0
3.0	0	0
3.5	0	0.4

Table 3.13 Results of packet loss ratio at DSSS rate 5.5mbps.

Hello interval	AODV	AODV with blackhole
0.5	0	0.4
1.0	0	1
1.5	0.6	1
2.0	0	1
2.5	0	0.4
3.0	0	1
3.5	0	1

Table 3.14 Results of packet loss ratio at DSSS rate 11mbps.

4. CONCLUSIONS

In this project we have compared normal AODV and AODV having blackhole attack. According to throughput graphs we can conclude that, at DSSS rate 5.5 mbps and hello interval range within 2.5s to 3.0s we get good results because here packet loss is low as compared to other result set. So, here we have tried to minimize the packet loss in the network having black hole attack.

REFERENCES

[1] Vipin Khandelwal, Dinesh Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs," IJARCET, Vol 2 Issue 4, April 2013.

[2] Thomas Edward Fogwell, et. al, "Location Based Analysis of AODV Performance in the Presence of Black Hole Nodes", IEEE, 2016.

[3] Vimal Kumar, et. al. "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network", Science Direct, Elsevier, vol 48, 2015.

[4] A. A. Chavan, et. al. "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack", Science Direct, Elsevier, vol 79, 2016.

[5] Md Raqibull Hasan, et. al. "An Effective AODV-based Flooding Detection and Prevention for Smart Meter Network", Science Direct, Elsevier, vol 129, 2018.

[6] Neelam Janak Kumar Patel, et. al. "Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 5 Issue: 5.

[7] Chaitali Biswas Dutta, et. al. "A Novel Blackhole Attack for Multipath AODV and its Mitigation", IEEE, ICRAIE-2014.

[8] Nidhi Purohit, et. al. Simulation study of Black hole and Jellyfish attack on MANET using NS3", IEEE 2011.

[9] Ramon Mart, et. al. "Performance comparison of routing protocols in VANETs under black hole attack in Panama City", IEEE 2018.

[10] M. S. Alkatheiri, et. al. "AODV routing protocol under several routing attacks in MANETs" , Communication Technology (ICCT), 2011.

[11] Alaa Hassan, Milena Radenkovie, "Simulation of Security Attacks and Preventions on AODV Protocol in NS-3," IEEE, 2014.

[12] On-demand distance vector (AODV) routing, RFC 3561, 2003.