# Simulation of AODV under Multiple Blackhole and Grayhole Attack in MANETS

Divya Khajuria
Department of computer science and engineering
Shri Mata Vaishno Devi University
Katra, India

Sudesh Kumar
Department of computer science and engineering
Shri Mata Vaishno Devi University
Katra, India

## ABSTRACT
Adhoc networks are infrastructure-less network designed for communication without aid of any centralised administration. An Adhoc network generally consists of fixed nodes. Another variation of Adhoc network is MANETs. MANETs consists of mobile nodes rather than fixed nodes. MANETs is self-configuring network of mobile nodes that can be formed anytime and anywhere. Due to dynamic nature of wireless medium, unpredictable topological changes, mobility and limited resource constraints, at network layer MANETs routing protocols poses various security challenges. AODV routing protocol is most popular protocol because of its low routing overhead and less algorithmic complexity. But it is vulnerable to various attacks because of lack of security system design, Blackhole and Grayhole attack being one of them. This paper evaluates performance of AODV under multiple Blackhole and Grayhole attacks.

## Keywords-
Adhoc, MANETs, AODV, Blackhole, Grayhole.

## 1. INTRODUCTION
In MANETs, nodes can communicate with their immediate neighbours as well with other nodes through intermediate neighbour nodes. MANETs can be formed on fly without any infrastructure. Because of wireless communication, mobility, lack of infrastructure, no centralised administration, dynamically changing topology there arises various security issues in MANETs routing protocol. Most of MANETs routing protocols lacks security. Because of open network malicious nodes can easily perform eavesdropping of the transmission of other nodes. In addition to this, malicious nodes can also modify transmitted packets or inject spoofed packets. There are two types of attacks –passive and active attacks. In passive attack, malicious nodes intercept the transmission but don't disrupt the network operation whereas in active attacks, attacker alters the data and disrupt network operation. Attacks occur frequently in routing protocols which are not designed to verify messages and protect data transmissions; so there is great need of securing routing protocols.

In this paper, Section 2 describes the related work. Section 3 deals with the theoretical description of AODV and section 4 explain the Blackhole attack and Grayhole attack. Simulation results are incorporated in section 5. Conclusion is discussed in section 6.

## 2. RELATED WORK
Rutvij *et al.* [4] provide a solution to mitigate Blackhole and Grayhole attacks in AODV based MANETS; it proposed a modified AODV viz. MR-AODV that isolates Blackhole and Grayhole nodes during route discovery phase by calculating PEAK value. PEAK value is obtained by adding three parameters- number of sent out RREQs, number of received RREPs and routing table sequence number to dynamically calculate PEAK value. Destination sequence number of received RREP is compared with tshis PEAK value to detect the existence of malicious nodes. The main advantage of this proposed solution is reduced routing overhead.

[5] has given a Black Hole Attack Prevention System in Clustered MANET scheme to prevent Black hole attack; it maintain a *Friendship Table* that specify the relationship of cluster head with its neighbour node. Source cluster head(S) broadcasts RREQ. S receives RREP. S selects the shortest and next shortest path according to hop count. S checks Friendship table for one-hop neighbour nodes. If neighbour node is a friend then Route data packet. Else Send false packets to the stranger. Invoke the trust estimator. If trust value is out of tolerable range, stranger is broadcasted as a Black hole. The scheme has limitations of increased routing overhead due to generation of *False* packets and also there is increased maintenance overhead due to extra table.

In Watchdog mechanism proposed by [6], every node keeps two extra tables, one is called pending packet table and another one is called node rating table. In pending packet table, each node keeps track of the packets which they sent. In node rating table, each node maintains rating of adjacent node. The last field of the node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node is considered as a misbehaving node, otherwise it is considered as a genuine node. Promiscuous node locally tells all the node of its wire-less range that particular node is misbehaving node. Discard RREP message coming from the misbehaving node. However, as the approach uses promiscuous mode, it consumes more energy, adds computational overhead to nodes and does not support directional antennas; adding to this, it adds overhead in terms of maintenance of two extra tables.

To reduce the probability of blackhole attack [2] proposed method that wait and check the replies from all the neighboring nodes to find a safe route. The source node waits for the responses including the next hop details from other neighbouring nodes for a pre-determined time value. After the timeout value, it first checks in the CRRT ( Collect Route Reply Table) table, whether there is any repeated next-hop- node or not. If there exists any repeated next-hop, it assumes the paths are correct or the chance of malicious paths is less. The solution adds a delay.

## 3. THEORETICAL DESCRIPTION OF AODV
AODV routing protocol is designed for the networks that consist of few to thousand nodes. AODV can handle low,

moderate and high mobility rates of nodes in network. AODV is a reactive protocol that has low routing overhead and high packet delivery ratio. That's why AODV performs better than proactive routing protocol such as DSDV. AODV is on demand routing protocol suitable for MANETS. AODV follows reactive approach in which route is established on the demand of source node, and intermediate nodes helps in transmission of packets. AODV uses destination sequence number to verify the recent path. AODV protocol can be summarized into route discovery and route maintenance process [10].

## 3.1 Route discovery

When a node needs to send packet to destination, it first checks its routing table and find whether route entry exist for destination in routing table. If yes then source node checks whether route is valid or not, if yes it simply transmits the packets. If no, then source node initiates route discovery process to establish a route to destination. Source node generate RREQ message and broadcast to their connected neighbours. Neighbouring node on receiving RREQ first determines whether they have received the same RREQ before, if yes, then discard it. If not, intermediate node respond to RREQ by either sending RREP or rebroadcasting RREQ to its neighbours after increasing hop count field. If intermediate node has fresh route to destination then intermediate compares the destination sequence number in received RREQ with destination sequence number stored in its routing table. If routing table sequence number is greater than or same as RREQ sequence number with smaller hop count, then intermediate node unicast RREP to source node, as intermediate node has most recent path to destination, otherwise intermediate node establish reverse path towards source node and rebroadcast RREQ. Eventually, RREQ will reach destination which will react with Route Reply message (RREP) which is sent as unicast, using the path towards source node established by RREQ. Therefore at the end of route discovery process, packets can be delivered from source to destination.

## 3.2 Route maintenance

Each node periodically broadcast HELLO message to determine the connectivity of link. After certain period of time if node does not receive any HELLO message, node will assume link is broken, then node will remove route entry for that link from its routing table and broadcast RRER (Route Error) message to notify neighbouring nodes about link breakdown and upstream nodes delete link which is not reachable.

# 4. BLACKHOLE ATTACK AND GRAYHOLE ATTACK

A Black hole node exploits the AODV routing protocol by setting destination sequence number higher, to advertise itself as having a valid and shortest route to a destination node, source node believes malicious node and start sending packets through malicious nodes. On receiving the packets, the malicious node drops the intercepted packets. In Blackhole attack, malicious node waits for the neighbours to initiate a RREQ packet. The malicious node on receiving the RREQ packet immediately sends false RREP packet with a modified higher sequence number. Source node believes that malicious node is having the fresh and shortest path to destination. Source node in turns ignores the RREP packet received from other nodes and starts sending data packets through malicious nodes. Thus, all the packets are directed towards malicious node. The malicious node doesn't forward any data packet to other nodes instead of forwarding it drops all the packets. This kind of attack is termed as Blackhole. Blackhole attack can be of single or multiple types. In multiple Blackhole attack, malicious nodes are more than one. Figure 1 below depicts the single Blackhole attack and Figure 2 below depicts multiple types Blackhole attack.

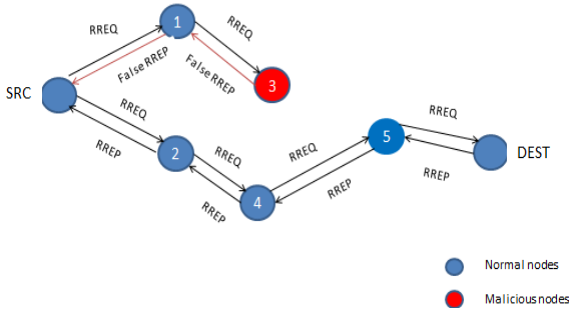



**Fig1: Single Blackhole attack**

In figure 1, Src represents source node, 3 represents malicious node, Dest represents destination node and 1, 2, 4, 5 are the intermediate nodes.

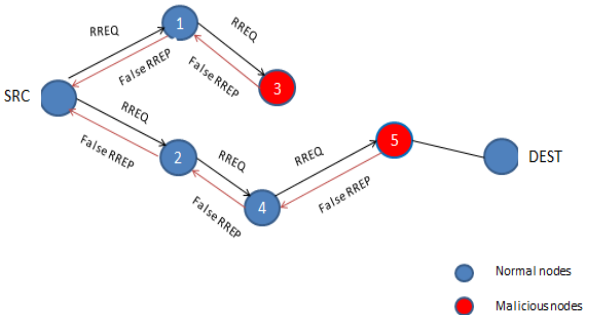



**Fig 2: Multiple Blackhole attack**

In above figure, node 3 and 5 act as malicious nodes which are sending false RREP having higher destination sequence number to source node.

In Grayhole attack, node initially behaves normal then turn to malicious node after some time. A Grayhole may exhibit its malicious behaviour in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour later. A Grayhole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult [11].

# 5. SIMULATION OF AODV UNDER ATTACKS

In this section, first experimental setup is described followed by performance metrics, network scenario, simulation results and analysis.

## 5.1 Experimental Setup

Experiments are performed using NS-2 (Ver. 2.34) simulator installed in Red Hat operating system. BlackholeAODV and GrayholeAODV are implemented to add Blackhole and Grayhole behaviours respectively. AODV.cc and AODV.h are modified to generate attacks. Random waypoint model is used

as the mobility model and Continuous Bit Rate (CBR) is used as traffic source; terrain area of 1100mx700m; packet size of 512 bytes; pause time of 2.0s; simulation time of 20s. The detailed Simulation parameters are presented in Table 1.

**Table 1. Simulation Parameters**

| Parameters | Value |
|---|---|
| Terrain Area | 1100mx700m |
| Simulation time | 20s |
| MAC | 802.11 |
| Application Traffic | CBR |
| Maximum Bandwidth | 2 Mbps |
| Routing protocol | AODV |
| Pause time | 2.0s |
| Data payload | 512 Bytes/Packet |
| Number of Nodes | 10 to 40 |
| Maximum Speed | 10m/s to 50m/s |
| Number of Sources | 1 to 5 |
| Number of Adversaries | 1 to 5 |

## 5.2 Performance metrics

The metrics used to evaluate the performance are given below.

### *5.2.1 Packet Delivery Ratio*

The ratio between the total number of packets received by destination nodes and the total number of packets generated by the source nodes.

### *5.2.2 Average End-to-End Delay*

Average time consumed by data packets to reach to respective destinations.

### *5.2.3 Throughput*

The number of successful bits per unit of time forwarded by the network from a certain source address to a certain destination.

## 5.3 Network Scenario

Network scenario created for evaluating AODV under Blackhole attack is shown in fig. 3. In this scenario node 0, 1, 6, 7, and 12 enclosed in pink box are source nodes and node 17 is the destination, whereas node 2, 3, 13, 18, and 19 enclosed in green hexagonal box are Blackhole nodes. Similarly, a same network scenario is created with nodes 2, 3, 13, 18, and 19 as Grayhole nodes for evaluation of AODV under Grayhole attack.

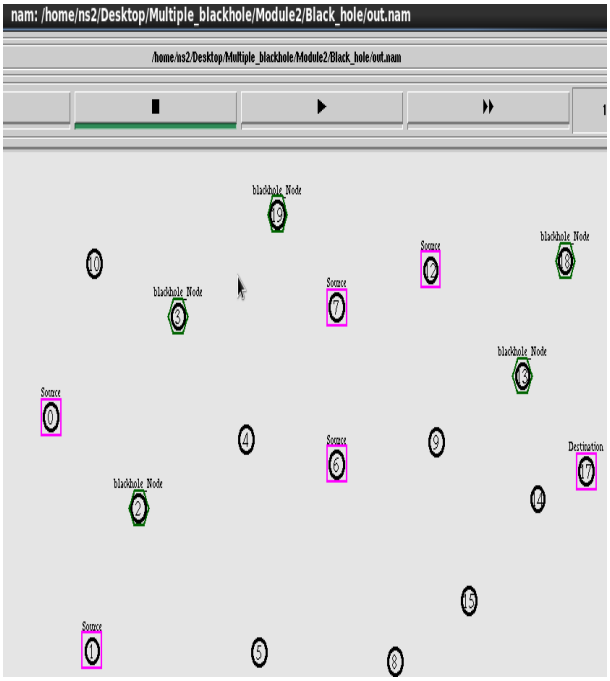



**Fig 3: Network Scenario**

## 5.4 Results

We evaluate performance of AODV under multiple Blackhole and Grayhole attacks by varying network size, mobility and number of malicious nodes.

### *5.4.1 Effect of Network Size*

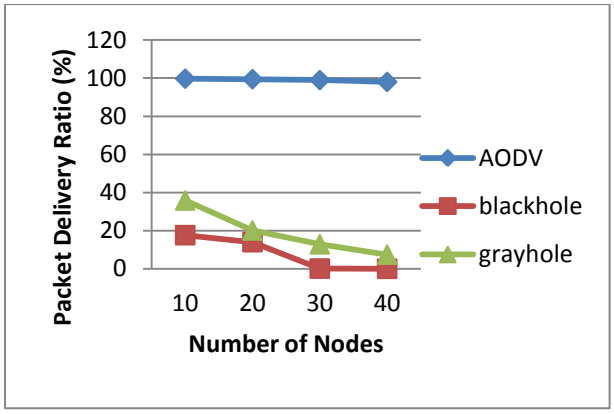
Number of nodes is varied from 10 to 40, keeping number of sources 5 and maximum speed of 50 m/s. Fig. 4 shows the behaviour of AODV under attack with varying the network size. From the analysis of graph it is found that PDR under Blackhole attack decreases significantly by 92% whereas PDR under Grayhole attack decreases by 80.08%. End to End delay under Blackhole increases by 18% and under Grayhole attack it is increased by 32%. Throughput under Blackhole decreases by 79% and under Grayhole it is decreased by 65%.

### *5.4.2 Effect of Mobility*

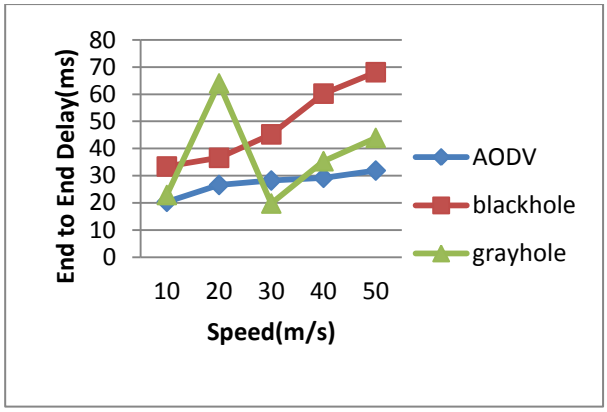
The speed is varied from 10 m/s to 50 m/s with network size of 20 and no of sources 5. In AODV under Blackhole attacks, PDR and threshold decreases by 95% and 79% respectively, and end to end delay increases by 72%. Whereas under Grayhole attack, PDR and throughput decreases 87% and 65% respectively, and end to end delay increases by 33%. The effect of mobility is shown in figure 5.

### *5.4.3 Effect of Multiple Malicious Nodes*

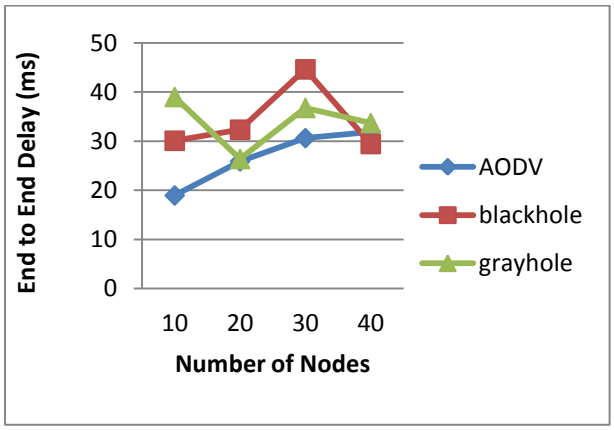
Fig. 6 depicts performance of AODV by varying number of malicious nodes from 1 to 5 with network size of 20, speed of 50m/s and number of sources 5. As number of malicious nodes increases, PDR under both attacks start declining.



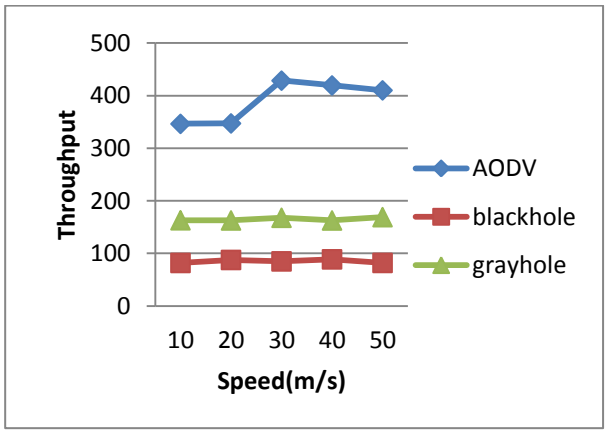

(a)




(b)

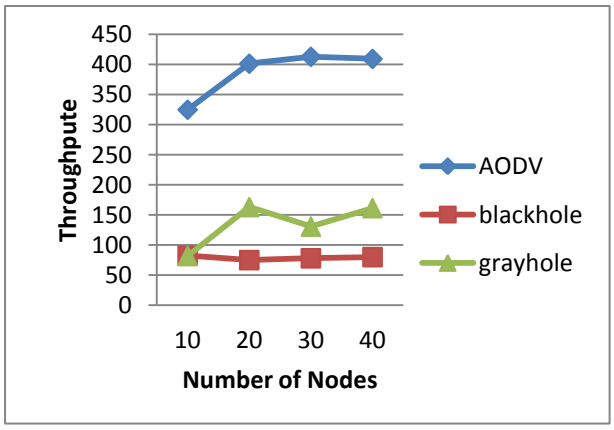



(b)



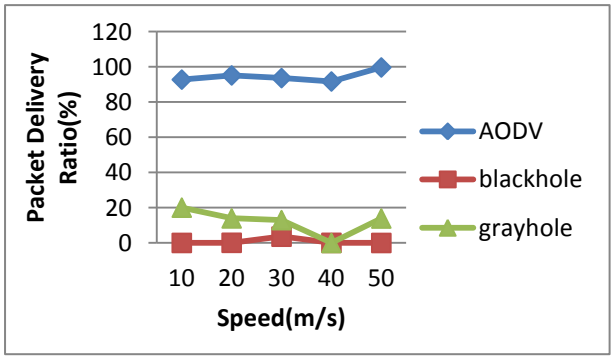

(c)

**Fig. 5: Effect of Mobility**




(c)

**Fig. 4: Effect of Network Size**




(a)

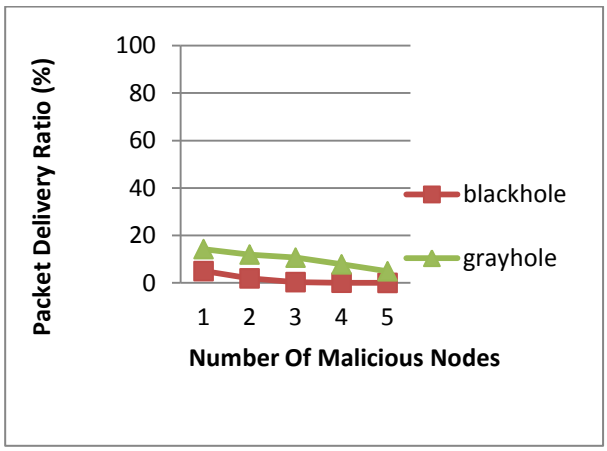



**Fig. 6: Effect of Multiple Malicious Nodes**

## 6. CONCLUSION

AODV routing protocol is vulnerable to both Blackhole and Grayhole attack due to lack of some security aspects in their design. In Blackhole and Grayhole attacks, malicious nodes send false routing information to source node during route discovery and disrupt normal data traffic in the network. In this paper, we simulate AODV under multiple Blackhole and Grayhole attacks. The performance of AODV is analysed under attacks. The result shows that the performance of AODV degrades under the attacks. PDR and throughput of AODV under attacks decreases whereas end to end delay gets increased. Blackhole and Grayhole attacks analysis on AODV

protocol highlights critical issues that need to be considered for the design of efficient security system for AODV.

## 7. REFERENCES

[1] Hongmei Deng, Wei Li and Dharma P.Agarwal, "Routing Security in Wireless Ad hoc Network", IEEE Communications magazine, Vol.40, No. 10, 2002, pp70-75.

[2] LathaTamilselvan and V Sankarnarayan, "Prevention of Black Hole Attack in MANET", Journal of Networks, Vol. 3, No. 5,2008, pp 13-20.

[3] Mohammad Al- Shurman, Seong - Moo Yoon And Seungjin park, " Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd Annual Southeast regional conference, 2004, pp 96-97.

[4] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks" In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing services(CPS), January 2012, pp.556-560.

[5] Ira Nath and Dr. Rituparna Chaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2 Issue 8, August 2012, pp. 113-121.

[6] Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre,"Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms", World Research Journal of Computer Architecture, Vol. 1 Issue 1, 2012, pp. 19-23.

[7] Rutvij H. Jhaveri,"MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV based MANETS", Wireless Networks Security on Signal and Communication Technology Springer, New York, 2011.

[8] J.Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation, Innovation lab, Tata consultancy services ltd., Kolkata, 25-27January 2011.

[9] Kalia Nishu and Munjal Kundan, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol", International Journal of Engineering and Technology, Volume-2, Issue-3, February 2013.

[10] Wang Huabin , Luo Zhongliang, " Research and Improvement of NS2- based AODV protocol in Adhoc Networks", Computer Era, No.5, 2011, pp. 12-14

[11] Jayedip Sen, M.Girish Chander, Harihara S.G., Harish Reddy, P.Balamuralidhar, " A Mechanism for Detection of Garyhole attack in Mobile Adhoc networks", Proceedings of the 6th International Conference on Information, Communications and Signal Proceedings(ICICS), ISBN-1-4244-0983-7,December 2007.

Moumita Deb, "A Co