# Black Hole Attack In AODV Routing Protocol

Miss. Divya[1], Dr. R.Gobinath[2]
[1]Research Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai,
Assistant Professor, Department of Computer Science, Prince Shri Venkateshwara Arts and Science College – Chennai.
[2] Assistant Professor, Department of Computer Science, VISTAS, Pallavaram, Chennai.

**Abstract :** MANET is the mobile ad hoc network used for connecting the mobile devices (nodes) and transferring the packets from source to destination node without connecting the nodes with the transmission medium. It is otherwise called as wirelessad hoc network or ad hoc wireless network. MANET is the self-configuring with less infrastructure network. MANETs undergoes different types of securities issues that disturb the actual performance and behaviour of the networks. One of the most dangerous attacks in MANET is the black hole attack, which results in dropping the data packets from network without transmitting the packet to the destination node. Ad hoc On-Demand Distance Vector (AODV) routing is a protocol used for mobile ad hoc networks (MANET). This paper implements the solution to the black hole attack in MANET using cache based IDS on AODV routing. This technique prevents the duplicate or unauthorised replies send by the attackers in the network.

**Keywords:** MANET, AODV routing, black hole attack, CBIDS.

## 1. Introduction

An ad hoc routing protocol controls how the nodes decide in which way to route the packets between the source and destination devices in a mobile ad hoc network. In ad hoc networks, the nodes are not familiar with their network topology but the nodes have to discover the topology. Each new node in the network initiates its presence and listens to their neighbouring node for broadcasting the announcement. It also learns about the adjacent node in the network to specify how to reach them while transmitting packets.

Routing is the process of finding the LINK (route path) from a source to destination node in the network. MANET contains three types of routing protocols namely reactive routing, proactive routing and hybrid routing protocol.

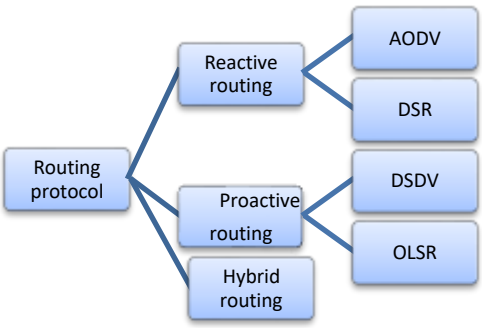


**Fig. 1 Routing protocol classification**

Ad-hoc On-Demand Distance Vector (AODV) is a reactive type of routing protocol. A Reactive protocol is otherwise called as on demand routing protocol because reactive routing protocol finds a path on demand by sending the Route Request packets among the network. Proactive routing protocols keep track of fresh lists

of destination nodes and their routes by distributing the routing tables periodically throughout the network. Hence it is called as table driven routing protocol. Hybrid protocol works with the combination of reactive and proactive routing protocol.

## 2. AODV Routing Protocol

AODV is the reactive routing protocol where the routes are determined only during the packet transmission from source to destination node. Moreover path is established only between the communicating nodes. Existing route establishment or fixed routing is not permitted in AODV routing because the route discovery process is initiated only when the needs to transmit the packet. AODV protocol is mainly used to detect the route break between the nodes in the network. The route break is identified if a node does not receive the message from its neighbouring node. AODV routing is similar to the Bellman-Ford distant vector algorithm. Designing AODV algorithm undergoes few main requirements namely low overhead, adaptiveness and resilience to loss.

**Route discovery and maintenance**

In the AODV routing, each node maintains the table that specifies to which neighbouring node the packet has to be send, in order to reach the destination. The main feature of AODV routing is the sequence number specified in the packet which ensures the route updates to reach the destination. AODV routing undergoes three types of messages namely RREQ, RREP, RERR. The RREQ is the route request packet which is flooded throughout the network to find the appropriate route to reach the destination node. The RREP is the route reply message transmitted by the destination node to the source node which represents the valid route to reach the destination. The RERR is the route error message which specifies the link break in the network.

Route discovery is initiated by transmitting the RREQ message and the route is established only when the RREP message is received by the source from destination node in the network. Multiple RREP messages may be received which suggest the different routes to reach the destination in the network.

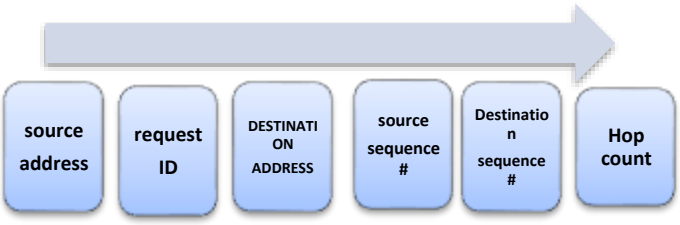


**Fig. 2 RREQ packet format**

The source node transmits the RREQ message to its neighbouring in the network which in turn broadcast it to the adjacent node and so on. The destination node or intermediate node (having route to destination) replies with the RREP message in response to RREQ. The RREP message received from the intermediate node is termed ad unwarranted route reply. Every RREP message is examined to check the route freshness by analysing the destination sequence number. Every time an intermediate node compares its sequence number with the sequence number in the RREP message. If the sequence number is greater than the number in RREP, then it is considered as the valid route in the network to reach the destination.

Each node in the network transmits the HELLO message to its entire neighbouring node for route maintenance. If any node does not receive the HELLO message from its neighbour, then it represents the

route breakage (link is down) and immediately transmit the RERR message to any node in the network. Finally the route break is cleared by analysing the RERR.

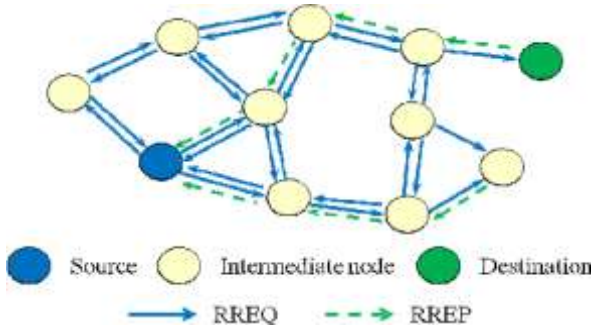


**Fig. 3 Propagation of RREQ and RREP**

## 3. Blackhole Attack In AODV

The only problem in MANET is the security attack due its feature like open medium and dynamic change in network topology. A black hole attack in MANET is due to the malicious node (hacker) present in the network. The malicious node creates the false route to the destination and attacks the data packets transmitted to the destination node in the network by simply dropping down the packets without forwarding it to the neighbouring nodes. In the black hole attack the attacker node detects and monitors the active route between the source and destination by tracking the destination address. This type of attack is said to be a kind of security threat which redirects the traffic to attacker node which is not the part of the actual network. The main characteristic of malicious node is to respond first to any of the adjacent node in the network.

As the source node transmits the RREQ message to its neighbour node, the malicious node will also receive the request message. It immediately responds the source node by transmitting RREP message before the other nodes transmit it. The RREP message transmitted by the black hole node is reached to the source node which allows the source node to transfers all the packets to the malicious node that is not the part of network. After receiving the packets from source node the black hole node simply drops the packet from network without transmitting it to the neighbour node in the network.

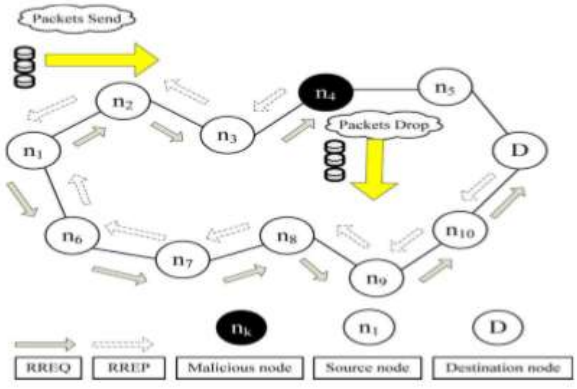


**Fig. 4 Packet dropping in black hole attack**

## 4. CBIDS AODV Protocol

The CBIDS AODV protocol is said to be the solution given to the black hole attack. This cache based IDS AODV protocol is the proposed technique used to solve the security issues in the MANET. This technique is implemented by changing the receive RREP message and creating the RREP caching which counts the second RREP message transmitted to the source node either from destination node or from malicious node. This cache IDS technique works by periodically removing the expired RREP messages from the list (route table) in the network which serves as the major solution to the black hole attack. The CBIDS AODV can be implemented with the help of network simulator NS2. The main purpose of NS2 simulator is to simulate the network traffic and supports multipath routing.

**Performance metrics**

**Packet delivery:**

The packet delivery ratio can be expressed by;

Packet delivery ratio=∑ No. of received packets / ∑ No. ofPackets transmitted * 100

**Packet loss:**

The packet loss ratio can be expressed by;

Packet loss ratio= (∑ No. of packets transmitted - ∑ No. of packets received) / (stop time – start time)

**Throughput:**

The throughput can be expressed by;

Throughput = (No. of receivedpackets * packet size *8) / simulation time

## 5. Conclusion

This paper explains the analysis and effect of black hole attack against AODV routing and CBIDS routing protocol in the MANET. The proposed method cache based IDS AODV routing protocol results in better performance in terms of packet delivery, packet loss and throughput while transmitting the data in the network.

## References

[1]. Dharman,V G. Venkatachalam "Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest"South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 321-329, ISSN No:

[2]. Gourav Ahuja, Mrs. Sugandha "A Review on Black Hole Attack in MANET" International Journal of Advance Research in Science and Engineering, Vol.No.6,Issue No.07,July 2017,www.ijarse.com,ISSN(0)2319-8354, ISSN(P)2319-8346.

[3]. Gurbir Singh, Nitin Bhagat "Removal of selective Black hole attack in Dynamic Source Routing (DSR) Protocol by alarm system" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-6, June 2015..

[4]. Dr. Gurjar, A. A. Dande, "BlackHole Attack in Manet's: A Review Study" International Journal of IT,Engineeriing and Applied Science Research(IJIEASR) ISSN: 2319-4413 Volume 2, No.3, March 2013i-Xplore International Research Journal Consortium www.irjcjournals.org.

[5]. Mrs.Jhansi,M Ms. K.RoopaDevi, Mr.B.Mukesh Chandra, "Effective Measure to Prevent Cooperative Black Hole Attack in Mobile Adhoc Wireless Networks" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 4, July-August 2012, pp.204-209.

[6]. Monika , Swati Gupta "Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 7 July 2015, Page No. 13268-13272.

[7]. Ms. Naveena, A Dr. K. Ramalinga Reddy "Dynamic Training Intrusion Detection Scheme for Black hole Attack in MANETs" International Journal of Engineering Research and Applications (IJERA) ISSN: 22489622 www.ijera.com Vol. 2, Issue 6, November- December 2012, pp.622-627

[8]. Ravindra Saini, P. Sunitha Devi" Malicious Node Detection in MANETs using Cooperative Bait Detection Approach and Trust Model" International Journal of Research and Scientific Innovation (IJRSI) |Volume III, Issue VIII, August 2016|ISSN 2321-2705.

[9]. Sapna Choudhary,Alka Agrawal "Threshold Based Intrusion Detection System for MANET using Machine Learning Approach" International Journal of Advance Electrical and Electronics Engineering (IJAEEE),ISSN (Print): 2278-8948, Volume-3 Issue-1, 2014.

[10]. SUSHIL KUMAR CHAMOLI, SANTOSH KUMAR, DEEPAK SINGH RANA, "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" Int.J.Computer Technology & Applications,Vol 3 (4), 1395-1399, ISSN:2229-6093.

[11]. Sushil Kumar,Deepak Singh Rana, Sushil Chandra Dimri, "Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET" International Journal of Computer Applications (0975 - 8887) Volume 124 - No.1, August 2015.