Prevention and Detection Techniques under Black Hole Attack in MANETS: A Survey

Nancy Mittal
M.Tech Student, Department of Computer Engineering, Punjabi University, Patiala, Punjab, India.

Lal Chand*
Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala, Punjab, India.

Abstract

Wireless mobile ad hoc network (MANET) is vulnerable to attacks due to lack of infrastructures. With the attacks they made the information not useful for users. In MANETS routing is one the special component and it has several routing protocols, which are affected from various attacks. Black hole attack is one of the well known security attack in wireless ad hoc network. Many researchers have purposed different techniques of AODV protocol to detect and protect from black hole attack. This review paper discusses the black hole attack on AODV and existing solutions of this attack on AODV protocol.

Keywords: MANETS (Mobile ad hoc networks), Black Hole Attack, AODV (Ad hoc On-Demand Distance Routing Protocol)

1. INTRODUCTION

Wireless networks provide connection flexibility between users at different places. Moreover, the network can be extended to any place or building without the need of a wired connection. Wireless networks are classified into two categories; Infrastructure networks and Ad Hoc networks. Wireless mobile devices are used in many application areas such as disaster relief, military services, conferences etc.

* Corresponding Author
Mobile Ad Hoc Network (MANET) is the independent arrangement of mobile nodes connected to each other by wireless linkages. Each node operates as an individual system as well as a router to advance packets further. The nodes are free to move around and establish themselves into a network. The link between each pair of the nodes may be more than one. This will allow an association of various links to be a part of the same network [1]. These networks do not require any permanent arrangement of base stations. This feature allows the connection of all the mobile devices fast and spontaneously. It is a peer-to-peer mode of operation that can significantly lengthen the distance of the wireless networks.

In MANET, nodes with in transmission range can communicate without any central coordinator directly over radio links. It is more vulnerable to various types of attacks due to open medium, dynamic topological configuration characteristics. Moreover, MANET features make routing process very difficult when compared to infrastructure based wireless networks. Therefore, it is a challenging task for MANETs to provide secure routing service with minimum overhead [3]. Hence, an optimal route has to be discovered to transfer packets from source node to destination node which passes through many intermediate nodes. The need for establishing an optimal efficient route
is the main responsibility of dynamic routing protocols where the network topology changes dynamically.

The rest of the paper is organized as follows: Section 2 presents a comprehensive review on AODV routing protocol. Section 3 presents Black hole attack. Section 4 presents a literature review on existing detection and prevention techniques used for black hole attack. Section 5 presents conclusion and future scope.

2. AODV ROUTING PROTOCOL IN MANETS

AODV is an on-demand (reactive) routing protocol where the source node (NS) needs to establish a connection with destination node (ND). AODV routing protocol is a special type of algorithm made for ad hoc mobile networks. AODV can perform dual tasks of unicast as well as multicast routing. It is called on demand routing because it will start forming the routes to a particular destination only when requested by the sender node; It broadcast the Route REQuest (RREQ) packets to neighboring nodes by initiates the route discovery process. To find the route, it must go through route discovery and route maintenance phase.

In route discovery phase, to obtain a route AODV uses RREQ and Route REPl'y (RREP) messages. When any intermediate node receives RREQ message, it starts to communicate with the source node by unicasting RREP message. When once the source node has received RREP message, it is ready to transmit data packets to the destination node. In route maintenance phase, the source node is informed about the link failure by transmitting the Route ERr or (RERR) message.

3. BLACK HOLE ATTACKS

Security is one of the main research topics in computer networks. One of the most famous attacks done by attackers is Black Hole attack. A black hole attack is an attack where the malicious node forcibly obtains the route with greatest sequence number and less hop count and subsequently overhears or drops all data packets. The wide usage of Ad Hoc networks in martial environment and other security sensitive usages have made the security a basic requirement for these networks. Because nodes participate in the routing process, they can destroy the network. As routing is based on some kind of trust between nodes, it provides a good chance for attackers to disorder routing process. It is of two types:

1.3.1 Single black hole attack

Single black hole attack is mostly and easily happened in the mobile ad hoc networks [5]. In Figure 3, node 1 is the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore, node 1 judges the route discovery process with completion, and starts to
send data packets to node 3. As all know, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

![Figure 3: Single black hole attack](image)

**Figure 3:** Single black hole attack [5]

### 1.3.2 Co-operative/collaborative black hole attack

Collaborative black hole node is that when there are two or more than two malicious nodes as in fig 4. The source node S broadcasted RREQ packet to all neighboring nodes which in turn forwards to next node if it is not the destination node. Both the destination node D and the malicious node BH1 sends RREP packet with largest sequence number and smallest hop count. Based on AODV protocol routing procedure, the source node S would prefer a shortest route of malicious node BH1 because of its smallest hop count 1 [6]. After obtaining the route, the malicious node overhears the upcoming packets or it may drop all packets which have been received. Cooperative black hole node BH2 is being introduced to strengthen the malicious activities and also to reduce the chance of finding the existence of malicious node BH1. Both malicious nodes BH1 and BH2 may partially overhear or drop the packets.

![Figure 4: Cooperative black hole attack](image)

**Figure 4:** Cooperative black hole attack [6]
4. LITERATURE SURVEY

4.1 Existing techniques for the detection of black hole attack:

1. Sina Shahab, Mahdieh Ghazvini, Mehdi Bakhtiar [7] suggests a new algorithm which enhances the security of AODV routing protocol to encounter the black hole attacks. This algorithm tries to identify malicious nodes according to nodes behaviors in an Ad Hoc network and delete them from routing. The results show some improvements in end-to-end delay and packet delivery rate in the suggested algorithm.

2. T. Poongodi, M. Karthikeyan [6] suggests a novel technique using Localized Secure Architecture for MANET (LSAM) routing protocol is proposed to detect and prevent co-operative black hole attack. Security Monitoring Nodes (SMNs) would be activated only if the threshold value is exceeded. If malicious nodes are detected, other SMNs in its proximity area are intimated to isolate the malicious nodes. With the LSAM algorithm, PDR is been increased by 27 % in the presence of 40 % misbehaving nodes and EED is greatly reduced from 0.9 to 0.3 %.

3. M. Rajesh Babu G. Usha [15] proposes a technique which is known as NHBADI, which uses Honeypot methodology to detect and isolate Black Hole attacks. Unlike existing techniques, the proposed Honeypot technique enhances the security of the MANET by reducing the network overhead. This proposed technique not only detects malicious Black Hole nodes but also isolates the vulnerable Black Hole nodes from the network. The proposed NHBADI technique reduces network overhead, normalized routing load and packet drop ratio.

4. Ali Dorri [16] proposed a routing approach to detect and eliminate cooperative malicious nodes in MANET with AODV routing protocol. A data control packet is used to check the nodes in the selected path by using an Extended Data Routing Information table and then all malicious nodes in selected path are detected, then eliminated from network. The proposed approach decreases packet overhead and network throughput is improved.

5. Arathy K Sa, Sminesh C Na [8] suggest the black hole detection schemes, which detect both single and collaborative attacks. They proposed D-MBH algorithm to detect single and multiple black hole nodes with the use of an additional route request with nonexistent target address, computes a threshold ADSN, creates a black hole list and invokes the proposed D-CBH algorithm. With ADSN, black hole list and next hop information extracted from RREP, then a list is made by D-CBH algorithm of collaborative black hole nodes. This algorithm reduced routing and computational overhead.

6. Siddharth Dhama, Sandeep Sharma, Mukul Saini [11] purposes the model in five cases with each one having 20 nodes where the protocol used is AODV, than after that the same is tested with BH node. Then again simulated 20 node model with solution that resulted in decreasing the effect of BH node. AODV operation has minimum packet loss but when a BH node is introduced in the network the packet
loss has increases to 88%. When we used the IDSAODV in the same network packet loss are decreased to 66%.

7. **Nidhi Choudhary, Dr. Lokesh Tharani**, [14] proposes a timer based detection approach for identifying black hole node. In network layer they proposed a Timer based method to overhear the next node action. As black hole attack causes great damage to the network performance, and it degrades further with the increase in the number of attackers in the network. Once this is the case the attack is done on the active flows by the attackers which results in packet drops, proposed method can be adopted.

8. **Pramod Kumar Singh, Govind Sharma** [17] proposed with uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, in other words, promiscuous mode means that if a node \( A \) within the range of node \( B \), it can overhear communication to and from \( B \) even if those communication do not directly involve \( A \). It does not require any database, extra memory and more processing power.

9. **Sagar R Deshmukh, P N Chatur, Nikhil B Bhople** [18] proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. This validity value is attached with the RREP message and is stored in route table at each node of active path. Whenever a node receives route request, if it is the intended destination or possess a legitimate route, then route reply message will be generated by setting value for validity bit in RREP (Here legitimate route refers to the route for which validity bit in route table is set). This RREP then will be sent back to its neighboring hop from which it obtained RREQ. The proposed route reply message differs in the validity value with the fundamental AODV route reply message. Proposed system neither requires heavy processing nor extra memory. With the addition of negligible overhead, black hole attack is prevented before actual data transmission phase.

**5. CONCLUSION AND FUTURE SCOPE**

MANET is vulnerable to various types of attack. Serious security problems in MANETs are - Black Hole attack. It is an attack where a malicious node sends a forged or fake RREP (route reply) to source node and initiates route discovery and prevent the data traffic from the source node. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs is done. Each technique has their own merits and demerits. In the end, it is concluded that the affect of black hole attack is negative on the network and we can reduce effect by using the above techniques. In future we can make effective algorithm to reduce the effect of black hole attack in MANET.
REFERENCES:


