Prevention of Black Hole Attack by using AODV for Wide Network

A.Anjaiah & Mounika Neela
St.Peters Engineering College,
anjaniprasad.adepu@gmail.com & mounika3028@gmail.com

ABSTRACT: AODV is a routing protocol that is designed for MANET and it is using the on-demand method to establish the routes between nodes. The main benefits of this protocol is establishments of desired routes to the destination. When the source node requires and it keeps the routes as long as they are needed. A black hole attack is a common attack that can be accrued in AODV protocols. In this kind of attack, the attacker can uses one or more malicious nodes which advertise themselves in the network by setting a zero metric to all the destinations causes all the nodes towards the data packets to these malicious nodes. The AODV is vulnerable against the black hole attacks due to having centric property. Where all the nodes to have share their routing tables for each other. A black hole attack is a severe attack that can be easily employed against routing in mobile ad-hoc networks. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. The Proposed Method PL2 has the modification done in AODV protocol for ensuring the security against the Black hole attack using NS2 Simulation.

I. INTRODUCTION

A network is a collection of two or more than two nodes or computer system which are connected together through wires or wireless. Wired network are those network in which computer devices attached with each other with the help of wire. The wire is used as medium of communication for transmitting data from one point of the network to other point of the network. Wireless networks are gaining popularity to its peak today, as the user wants wireless connectivity irrespective of their geographic position. Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them.

The general network is the network that is included LAN and WAN types of networks. These networks are mostly used in schools, colleges and organizations etc.

One of the main active attacks is Black hole attack which takes place in network layer. In Black hole attack, a malicious node or group of malicious node drop the entire packets between source to destination. In this project, we attempt in analysing and upgrading the security of the AODV routing protocol against Black hole attack. AODV is an on demand, dynamic routing protocol and consumes less bandwidth than table driven protocol. Protecting against Black hole attack, additional commands are included in AODV.

Our proposed method is a PL2 method is a combination of postlude and prelude control messages. Source based detection method is used to mitigate the Black hole attack is possible by customizing the original AODV. The simulation is done in ns2. This analysis was done on the basis of certain parameters such as route Throughput, Packet-Delivery Ratio, Average end-end Delay, Drop rate.

II. LITERATURE SURVEY

Sun B et al [1] used neighborhood based method to detect malicious node in the network. In detection procedure neighborhood set of information is collected, further collected information is used to determine whether there Black hole attack exists. In response procedure source node sends Modify-Route-Entry (MRI) control packet to destination node to build a correct path by modifying entries of intermediate nodes. This simulation fails to detect forged fake RREPs.
Tamilselvan T [2] proposed a solution based on time based threshold detection scheme. The main concept is setting timer for collecting all other RREQ from other nodes after receiving the first request. Collect Route Reply Table is used to store the packet’s sequence number and the received time. In Route Discovery, the validity of route is checked based on the arrival time of the first request and the threshold value. This simulation shows that a higher packet delivery ratio is obtained and end to end delay might be increased when the malicious node is away from the source node.

Djenouri D et al [3] proposed a solution based on Random two hops ACK and Bayesian detection scheme. In monitor phase two hop ACK used to check the reliability of the intermediate node. In detection and removal process, Bayesian approach is used for node accusation. This simulation is efficient for all types of packet drops and has reduced overhead. This solution is not suitable for multiple Black hole attack.

DPRAODV [4] scheme has Detection, Prevention and Reactive AODV scheme. The solution is based on the validity of the RREP sequence number. If the RREP sequence number is higher than threshold value, that node is added to the Blacklist. Further receive reply from that malicious node is ignored. This simulation shows that improved packet delivery ratio at the cost of higher routing overhead.

Tsou Po-Chun et al [5] designed unique solution named Bait DSR based on Hybrid Routing scheme. Initially the source node sends Bait RREQ, having destination address which does not exist. This bait RREQ can attract the forged RREP and can remove Black hole nodes. This simulation results show increased packet delivery ratio and acceptable overhead.

III. OVERVIEW OF AODV PROTOCOL

The Ad-hoc on demand Distance Vector routing algorithm is a designed for ad hoc mobile network. It’s a routing protocol i.e. determine the appropriate path from the source to destination. The AODV is capable to route both unicast and multicast. These protocols are broadly divided into two categories [9].

a) Table-driven routing protocols or proactive routing protocol.

b) Source-initiated on-demand driven routing protocols or reactive routine protocol.

Table-driven routing protocols are also known as proactive routing protocols. The proactive routing protocol are maintain table of all routing information. These protocols desire to maintain unique, exact and all routing information in the network. All the nodes exchange routing information periodically and also there is even a minor change in the network topology and thus, every node in the network maintains one or more routing table are stores routing information about every other node in the network [10]. Source-initiated on demand driven routing protocols are also known as reactive routine protocol. AODV is a reactive routing protocol used to search a route between source and destination and establish new route and give new route path. In this order it is manage route and different types of link is establish, information are exchange. Its find route when necessary [11]. The drawback of this routing protocol is delay due to route discovery.

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Request ID</th>
<th>Source Sequence Number</th>
<th>Destination Address</th>
<th>Destination Sequence Number</th>
<th>Hop count</th>
</tr>
</thead>
</table>

RREQ FORMAT

IV. BLACK HOLE ATTACK

Black hole attack is a Denial-Of-Service attack that could easily happen in wireless network. To carryout Black hole attack in the network, a malicious node waits for the neighbouring node to send RREQ messages [10][11]. After getting RREQ messages, it sends fake RREP at once, as it has route over destination without checking routing
table by assigning high sequence number. So requesting node assumes that Route Discovery process is completed and starts transmitting data packets over that malicious node, without knowing about malicious activity. Black node drops the incoming entire packets between the source to destination, instead of transmitting to destination. As a result the source and destination node unable to communicate with each other. Since AODV treats RREP messages having higher sequence number to be fresher, the malicious node always send the RREP having higher sequence number [12].

![Fig.3 Black Hole Attack](image)

**Detection of Black Hole Activity**

Initially, data packets are divided into equal parts as Data (1… K) Where K=ceiling of (n/w).Where n is the number of data and w is the window size. Apart from the source, destination, some intermediate nodes are assigned as monitor nodes, given powers to overhear data packets and watching other intermediate nodes. After Route Discovery process, monitor(S, D, NNR) nodes are broadcasted to all other NNR-Next Nodes in the Route. Source node sends prelude (S, D, ni) message with every equal block of data and waits for special type of acknowledgement as postlude.

**Black Hole Removal Process**

In Black hole removal process, source node sends query BQ (S, D, NRREP, ni) to monitor node to find out malicious node. NRREP is the ID of the node sending RREP to source. In response monitor nodes sends back result to source node. If source node receives result before a particular time TRES, predicted that the particular monitor node itself is a malicious node. So Source node depends on other monitor node’s results to build a secured path. Based on monitor nodes result, source node starts votecount. Votecount is a count, for not forwarding the data packets of the particular node, when it receives from other node. If votecount of the particular node is greater than the threshold value, the source node confirms that the node as a Black hole node and will be listed in Blacklist. Threshold value is a variable depends on the size of the network. As source node knows the location of the Black hole nodes, it ignores the RREPs from these nodes. The flow chart for detailed process is as shown in Fig.4.

![Flow chart](image)
VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed PL2 method. PL2 is a source, neighbour, time based and modified AODV routing protocol to mitigate Black hole attack. We simulated our proposed solution using ns-2 and compared our modified AODV with original AODV in terms of packet delivery ratio and throughput. Simulation results shows that the proposed method has good performance against Black hole attack and not much overhead. This solution holds good for gray hole attack also. In our future work, we may propose a feasible solution which will strengthen original AODV against multiple Black hole attack.

REFERENCES

Anjaiah Adepu received B.Tech. in computer science and engineering from JNTUH Hyderabad and M.Tech. in computer science and Engineering from JNTUH Hyderabad. He is currently working as Asst. Professor, Department of Computer Science and Engineering at St. Peters Engineering College, Hyderabad, TS, INDIA. He is currently working toward the Ph.D. degree with the Department of Computer Science and Engineering at Shri Venkateshwara University, Gajraula (U.P.) He is having 12 years of Teaching experience, published more than 20 papers in National/International Journals/Conferences. He is a member of IAENG (International association of Engineers), ISOC (Internet society of India), CSI (Computer Society of India). His areas of research include Adhoc sensor networks, Information security, Internet of Things, Cloud computing.

Mounika Neela received B.Tech. in computer science and engineering from JNTUH Hyderabad and M.Tech. in computer science and Engineering from JNTUH Hyderabad. She is currently pursuing Mtech, Department of Computer Science and Engineering at St. Peters Engineering college, Hyderabad, TS, INDIA.