A Novel Approach for Detection of Blackhole Attacks

Ankita V. Rachh¹, Yatin V. Shukla², Tejas R. Rohit³

¹(C.S.E. Department, B.H. Gardi College of Engineering & Technology, India)
²(C.S.E/I.T. Department, B.H. Gardi College of Engineering & Technology, India)
³(Computer Department, Darshan Institute of Engineering & Technology, India)

Abstract: The MANET (Mobile Adhoc Network) is a wireless distributed network. It is formed by group of autonomous mobile nodes without any infrastructure like access points. Every node of MANET can acts as router as well as host. It has a basic characteristic of dynamic topology, it means nodes can enter and leave network any time. MANET is vulnerable to many security attacks. Black hole attack is most occurred attack in MANET and very hard to detect which is performed on network layer. Black hole attacks are classified into two types. In single black hole attack, one malicious node will change the route of source to destination and wrong path of malicious node will follow. In collaborative black hole attack one malicious node records packet at one end and send to another malicious node at other end. Black hole attacks are active attacks. In this paper, we propose a solution for detecting black hole attack. Our protocol’s name is EBAODV (Enhance Black hole AODV). In this approach, leader nodes are used for detecting black hole nodes.

Keywords: AODV, Black hole attack, EBAODV, MANET

I. INTRODUCTION

The introduction MANET is self organized distributed wireless network. Each node of network is Adhoc, without any infrastructure. In MANET, all wireless nodes can communicate with each other directly. In infrastructure based network all nodes can communicate with access points only. Fig. 1 shows infrastructure network. In MANET each and every node can change their position frequently, so track issues of MANET is good research. Fig. 2 shows Mobile Adhoc network. The basic requirement of MANET is source and destination must be within source’s transmission range. If destination is outside the source’s range then intermediate nodes behave as routers.

In MANET, due to dynamic topology link break between routes is occurred. When there is a link break in route, then local route repair occurs [5].

In this paper, we first give introduction of routing protocols in section II. Section III gives information of AODV protocol. In section IV we focus on black hole attack and comparative study of their solutions. Next section focuses on our proposed approach.

II. ROUTING PROTOCOLS

The main goal of routing protocol is to set up an optimal route from source to destination having higher packet delivery and minimum delay [18]. There are three basic types of routing protocols.

Fig. 3 Routing Protocols
1.1 Proactive Routing Protocol

The proactive protocol is a table-driven protocol as every node maintains a route table. Mobile nodes broadcast their routing information to their neighbors. The advantage of proactive routing protocol is network status can be immediately reflected if the malicious attacker joins. The disadvantage is overhead rises as network size increases [9]. DSDV (destination sequence distance vector) and OLSR (optimized link state routing) are proactive protocols.

1.2 Reactive Routing Protocol

The reactive routing protocol is an on-demand routing protocol as it transmits data packets when needed. The advantage of reactive protocol is wasted bandwidth induced from cyclically broadcast. The disadvantage is passive routing method leads to some packet loss [9]. DSR (dynamic source routing) and AODV (Adhoc on demand distance vector) are reactive protocols.

1.3 Hybrid Routing Protocol

Hybrid routing protocols combine proactive and reactive protocols. ZRP (Zone routing protocol) is the best example of hybrid protocol. In ZRP, the whole network is divided into various zones. Intra zone routing protocol is proactive and inter zone routing protocol is reactive [1].

III. AODV PROTOCOL

AODV (Adhoc on demand distance vector) protocol is reactive protocol, so route is established when it is required. AODV performs in two steps.

3.1 Route Discovery

Route discovery is a process of finding a route from source to destination. There are three control messages used for establishing a routing path. Route Request (RREQ), Route Reply (RREP), and Route Error (RERR).

![Route Discovery Diagram](representing RREQ)  
![Reverse Path Setup Diagram](representing RREP)

Route discovery broadcasts RREQ message into the network. A node receives RREQ will check its routing table to see whether it has a path to the requested destination [10]. RREP message is used to reply the request message. If the source node receives multiple RREP messages, it will select the shortest and freshest path. If there is no route to the destination, RREQ is forwarded and it keeps the reverse path to the source node [10]. AODV uses sequence number to find a fresh route. A node which receives RREQ will send RREP if it is either destination or if it has a route to the destination with a higher sequence number [14]. If any node receives RREQ which have already processed then it is discarded. Shorter and fresher route is selected from source to destination and then actual data packet transmission is started. After some time, source receives RREP having same or higher sequence number with small hop count. It will update the routing and now this will select as the best route.

3.2 Route Maintenance

Route maintenance commences when any link breaks in source to destination route. Source node will receive route error (RERR) message then it starts route discovery again for finding a new route. A routing table entry expires if not used recently [2]. Another way to repair the route is local route repair. Repairing node broadcasts RREQ and waits for RREP message. If repairing node fails in receiving RREP it broadcasts RERR to inform other nodes that the link is broken.
IV. BLACK HOLE ATTACK

Black hole attack is denial of service (DOS) attack. It can be classified into two types. Single black hole attack and Collaborative black hole attack. Occurrence of single black hole attack in MANET is very common and very hard to detect. In single black hole attack one malicious node is there. It claims itself that its path is shortest to destination. This node drops routing packets instead of forward packet to destination [9]. In collaborative black hole attack minimum two malicious nodes are there and transfers packet from one malicious node to another. The aim of black hole attacker is to attract traffic towards it and block data packets by dropping them [16].

In Fig. 7 source node S starts route discovery by sending RREQ message. Malicious node M also receives RREQ message, it sends false RREP message having higher sequence number. Source node S select route from malicious node M. Node M drops packets instead of forwarding and packet delivery ratio of protocol degrades.

In collaborative black hole attack malicious nodes are collaborate together and suspect the route. At least two malicious nodes are required for collaborative black hole attack. It is also known as cooperative black hole attack. Two malicious nodes establish direct wireless link. First malicious node establishes data transmission route and second malicious node drops transmitted data packets [11]. In case of TCP packets, source will come to know about malicious node because it will not receive ACK. In case of UDP packets, source will never come to know about malicious node as UDP do not send ACK [21]. Table I summarizes comparative analysis of black hole detection methods.

<table>
<thead>
<tr>
<th>Research Paper</th>
<th>Approach</th>
<th>Performance Matrices</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black hole effect mitigation method in AODV routing protocol [15]</td>
<td>Enhance AODV</td>
<td>PDR using AODV,ERDA and EAODV</td>
<td>Extra route reply message is used from destination and gives better performance.</td>
<td>Throughput and delay’s results are not specified.</td>
</tr>
<tr>
<td>Securing Routing table update in AODV routing</td>
<td>ERDA</td>
<td>PDR, NRL ratio and delay</td>
<td>Improves process of updating routing entry.</td>
<td>Does not work with outlier detection</td>
</tr>
</tbody>
</table>
V. PROPOSED WORK

In our proposed solution EBAODV, leader nodes are created first. Leader nodes are used for detection of malicious nodes. From source node RREQ is generated. At that time one timer is used for measuring current time. We can assume any expired time (here 20ms). If RREP received before expired time then one fake packet will send to the destination, this packet is not original data packet. After that if acknowledgement (ACK) receives then original packet will send by source node. If ACK not receives it means packets are dropped. If no. of dropped packets are more than threshold value (here 10) then leader nodes will send block message to all its neighbors. Block message contains id of malicious node. All intermediate nodes receives table having black hole node. Now, again new RREQ message is generated for route discovery.

5.1 Flowchart of EBAODV

![Flowchart of EBAODV](image)
VI. Conclusions And Future Work

Security is the important issue of routing protocols of MANET. Many attacks are vulnerable to AODV routing protocol of MANET. In AODV routing protocol, nodes having highest sequence number is selected for fresh and short route. In black hole attack malicious node will accept RREQ from source node and drop the packet instead of sending to the destination. In this paper, comparative analysis of black hole detection techniques are also discussed. We propose a new approach EBAODV (Enhance Black hole AODV) which uses leader nodes for detection of black hole. In our approach PDR (packet delivery ratio) and throughput will increase than original AODV.

As part of our future work, we will implement our approach in NS 2 and we will measure PDR, throughput and end to end delay using different parameters.

REFERENCES


