An Improved Performance of MANET using AODV Protocol for Black Hole Detection

Komal*
CSE Department, GGITC, Ambala, India
Komalbhatti27@yahoo.com

Sonam Dhawan
CSE Department, GGITC, Ambala, India
Sonam.dhawan306@gmail.com

Abstract: Routing attacks have been identified for single path routing in wireless ad hoc networks. The effects of routing attacks on multipath routing have not been addressed so far. In this paper, an approach have been proposed to mitigate the black hole attack using AOMDV (Ad hoc on Demand Multipath Distance Vector) routing protocol. Some improvements have been made in AOMDV protocol. These improvements make the protocol robust against black hole attack along multipath route discovery process. The performance of proposed approach has been investigated to further reduce the overhead as described in this paper.

Key words: Network security, Route discovery, AOMDV, MANET, Multipath, RREQ, RREP.

INTRODUCTION

MANET is becoming popular day by day. The reason is the need of communication in mobile needs. Due to its popularity its security problems are also increased. One of the security attacks is black hole attack.

Black hole attack malicious nodes get a chance to attack during route discovery process. A black hole means that one malicious node utilizes the routing protocol to claim itself of having shortest path to the destination node, and drops routing packets and does not forward packets to its neighbors [1]. A single Black hole node can easily attack on mobile Ad hoc networks [2]. There is various detection schemes for detecting single black hole, but failed when cooperative black hole attack occurs. Cooperative black hole attack means malicious nodes act in a group [3] [4]. In this attack, one malicious node receives data and forwards it to other malicious node instead of forwarding it towards destination [5]. The methods proposed earlier were categorized under two categories. The first category specifies the classification of different routing protocols such as AODV, OSDV, DSR to avoid black hole attack in MANET and the second category is of those which adopt an extra monitoring system such as watchdog, confidant protocol or intrusion detection system. [6][7][8][9]

The proposed approach of the system is based upon AOMDV (Ad Hoc On Demand Multipath Distance Vector). This approach detects black hole and discover nodes disjoint multipath which decrease the overhead of a specific node. In this paper the related work is explained in the next section and the proposed system is introduced in the 3 section.

II. HISTORY

In the previous work, effect of multiple black hole nodes on multipath routing has not been addressed so far. So Problem can be defined as:

- To recognize paths having black hole nodes.
- To select a safe path when multiple paths are available.

III. RELATED WORK

a. CAODV free black hole attack in MANET

The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs)[11]. A method was used to detect the black hole attack which was given by Watchara and Sakuna based upon the credit based mechanism [8]. To understand this method let us get some terms to know:

1) Hop Count: It is the number of nodes from which a node is far away from the destination node.

Here, hop count for the S (sender node) = 4 and for X =3

Table 1. Initial value credit for every node
entry must be added in trust table. This process will repeat until RREQ [10] is received by destination node. This modified protocol improves the delivery ratio by 15%, end to end delay is improved by 55% as compared to original AODV.

4) Methods of Mohammad al Shurman and Seong Moo Yoo:

The methods given by these researchers provide the verification and authenticity of RREP by the sender node. It utilizes the network redundancy, because a packet may follow many destination paths to reach to the destination. It would store all the RREP packets until a safe mode is identified. There will be some common hops of two or more replying nodes. Out of them, a source node recognizes the safe route. If there will be no shared node, then sender will wait for more RREP until a route is identified by the shared node or route time expired [9].

Second method depends upon the sequence number increased of a packet i.e. the value of the next packet must have a greater value than sequence number of current packet which a node is received. The routing protocol keeps the record of last sequence number to verify whether the same packet is already being received or not. Therefore, every node keeps the small sized tables having sequence number of last packet sent to each node and LSPN received from every node. Tables get updated time to time by arriving or sending of packets. When RREQ is reached to destination then RREP is initiated for the source containing LSPN received by the source. The solution thus obtained is reliable to identify the suspicious reply [9]. LSPN is included in every packet by base protocol therefore no overhead added to the channel.

IV. PROPOSED SYSTEM

The proposed system is based upon AODV protocol. Multiple black holes can be avoided by this protocol if it immediate replies to the RREQ. There will be multiple paths but the protocol chooses only one path. The proposed protocol has different message format and type:
A. Modification done in RREQ:

A new field called First hop is added in the RREQ packet [12]. The address of the first hop is contained in this field after it left the source node, then link disjoint multipath are created by ignoring the RREQ arrived by the same node. If the value of first hop is matched with the last RREQ received then we ignore it and only first value will be considered. This method is explained with help of figure 4.

In the figure, initially there is no value of first hop field; when RREQ packet is initiated by S. When RREQ sent to node D from both the nodes B and C, then D will find that the first hop fields of both have the same first hop address. It will choose the node on the basis of first come first come and B reached earlier than C, then it will discard node C.

B. Modification in RREP:

In RREP packet, an additional field is added called originator as shown in figure 5. This field claims that the node it has right path to destination as this field contains the identity of node. This node can be intermediate node or the destination node itself.

Here is the originator showing the use of ‘originator field’ in the figure 6.

In this figure, B is the Destination sending RREP to backward path, as RREP’s originator is destination itself, so the address of destination B will contained in the originator field. In this example node E is also having a route to destination. Address of A is contained in the originator filed of A’s.

C. Legitimacy Table:

Each node is maintaining a legitimacy table having two values for every node in the proposed protocol. Here is a legitimacy table to understand its field and value of fields.

<table>
<thead>
<tr>
<th>Node</th>
<th>Selection</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>B</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

In this table three different fields are there: (1) how many times a node has been selected during a node have been selected during its path discovery is shown in ‘selection field’. (2) How many times the path containing this node was successful is shown in ‘success field’. Legitimacy ratio indicated the performance of node to perform function. If there is chance of node being malicious then there will be less legitimacy ratio.
D. Route change of packet:
The additional packet which is used by the proposed approach is route change packet. It consists of three different fields (1) source address, (2) destination address and (3) bit change. For change of route to other path, nodes use it to inform the first node in backward path, which has legitimacy ratio higher than the previous one; Flushing of all the other nodes in backward route.

![Route change packet](image1)

First node in the backward will set the bit to 1, so that other nodes will not switch their route to another path in the backward route.

E. Modification into the routing table:
In the routing table three more additional fields are added: (1) first hop, (2) valid hop and (3) count as shown in table given below:

![Routing table](image2)

Table III: Routing table with three additional fields.

<table>
<thead>
<tr>
<th>Destination Sequence Number</th>
<th>Destination IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First hop</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Valid Bit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Count</strong></td>
<td></td>
</tr>
<tr>
<td>Hop Count</td>
<td></td>
</tr>
<tr>
<td>Next Hop</td>
<td></td>
</tr>
</tbody>
</table>

1) First hop is the first field which will store the value of first hop after the RREP is initiated by the node. It avoids the loop in the formation of path.

2) Valid Field is the second field which has three values 0, -1 and 1 only. Different value have different significance:
   i. Value 0: it shows the path to the destination through next hop which may not be correct.
   ii. Value 1 specifies that there is no malicious node in between the path.
   iii. Value -1 indicates that there is no entry closed for transferring the data.

3) Count Field specifies that the number of RREP received having the same sequence number for the entry but its value will be -1 if the RREP arrived after creating the entry.

Valid bits -1 = path not taken for transferring data
0= path may not be correct
1= path is free from malicious node and is correct.

V. RESULTS & ANALYSIS BASED ON PERFORMANCE

A. Metrics used for performance analysis are network load, packet end to end delay and network throughput.

1) Packet end to end delay: It is the average time in order to traverse the packet inside the network. It includes the time from packet generation to the time till the packet is received by the receiver. It calculates in seconds. It has:
   a. Delay introduced due to routing activities.
   b. Transmission time
   c. Delay of network including buffer queue.

2) Network Load: The total traffic which is received by the total network is called network load. The total network quantity in the whole traffic is indicated in bits/sec. Due to the large size of data packet it rejected the data traffic without queuing as it does not have any layer to handle this.

3) Throughput: The ratio of data received to the time at which the last packet is received is called throughput. Total data traffic is represented by bits/sec. The number of various changes affects the throughput like limitation of bandwidth, limitation of power and topology changed; also the unreliable communication affects the throughput parameter [10].

B. Tool used:
For analyzing the performance of proposed approach Mat-lab [11] is used. It is powerful computing system used for handling the calculations involved in scientific and engineering problems. With the use of Matlab one can solve many technical problems faster than other techniques like java, C, C++ etc.

C. Experimental Setup:
For the experimental setup we have two different cases consisting of seven mobile nodes and 20 mobile nodes at a constant speed of 10m/s.
In the first case RREQ is initiated by source node and discovery of path. Nodes are varied and time for experiment is taken as 750sec. Experimental area between 80*80 to 100*100. Packet interval time is taken as exp(1) and size of packet is exp(1024) bits. In the case having seven nodes, the first node is taken as the source node and the last node is taken as destination node and one node will be the black hole node. Similarly, for the second case having the 20 nodes, one is the source node; one is the destination node and two black hole nodes.

2) Packet loss: The number of packet lost during the transmission is known as packet loss. It is less in starting and after a small interval of time its starts increasing.

D. Results:

1) Black hole detection: A threshold trust level value is varying according to the network as shown in figure 10.

Nodes having trust value below the threshold level are shown as black hole nodes in the figure 11.
3) Packet received: The number of packets received per unit time by the receiver. In simple AODV packet received are 20 packets/unit time. But in our system the packets start receiving increase from the start. There is 8% increment in the number of packets received per unit time.

4) End to end delay: time included from packet generation by sender till to the packets received by the receiver. The percentage of being in a severe condition in end to end delay is 6-10% in case of AODV protocol without any improvement. On the basis of analysis of result and research the conclusion is that AODV is more vulnerable to black hole attack when there is no requirement applied.

By using our system the end to end delay can be reduced to 4-5% as shown in experimental result.

VI. CONCLUSION
During this work period, we have faced many challenges and behavior of security threats in MANET and tried to improve the performance of AODV protocol against this Black Hole attack. In our work, we analyzed black hole attack against the performance parameters of throughput, end to end delay and network load. The percentage of state of being severed in end to end delay is 5-10% in case of AODV without any improvement. Based on my research and experimental results the conclusion is being drawn by the analysis is that the AODV is more vulnerable to black hole attack when improvements are not applied as explained earlier.

REFERENCES

Fig. 12 (a) Packet loss in Simple AODV, (b) and in our proposed system

Fig. 14) Packet received (a) in simple AODV and (b) in our system

Fig. 14 End to end delay