Malicious Node Attack Preventer (MNPAP) Approach for Mobile Ad-hoc Networks (MANET’s)

Raj Mohan Mumgai  
M.Tech (WMC) Student  
Dehradun Institute of Technology  
Dehradun, India

Sandip Vijay  
Professor & HOD  
Department of ECE & AEI  
Dehradun Institute of Technology, Dehradun, India

ABSTRACT
A Mobile Ad-hoc network is a heterogeneous network. They have very particular features such as high mobility, multi-hop routing, open system and the absence of any fix infrastructure. An ad-hoc network faces different type of security attack. In this paper, we discuss our implementation of the AODV protocol extension namely Malicious Node Attack Preventer (MNPAP). AODV extension mechanism improves the AODV behavior. MNPAP used the reserved field of RREQ and RREP packet format. MNPAP implements security in AODV against black-hole and gray-hole attacks. Analyzes has been done based on PDR, throughputs and delay of the node selected by doing simulation on Qualnet network simulator.

General Terms
Security

Keywords
AODV, MNPAP, Non-Trustworthy, Trustworthy, Qualnet

1. INTRODUCTION
The wireless arena has been experiencing exponential growth in the past decades. In the last few years we have seen the multiplication in introduction of wireless communication technologies. Wireless technologies are being widely used today across the world to support the communication needs of a huge numbers of end users and hosts.

There are two different models for enabling wireless communication between two users [3]. The first approach is cellular network infrastructure and the second one is radio-to-radio multi-hop hopping commonly known as a Mobile Ad-Hoc Network (MANET) [2].

Many secure and non secure routing protocols for mobile ad-hoc networks have been proposed. The focus is on routing at a non-geographical scale and the classifications proposed in [1], for which a flat network structure is chosen.

The Internet Engineering Task Force (IETF) MANET working group introduced many different experimental Request for Comments (RFCs) [2] that specify flat routing protocol: Ad-Hoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR), Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), and OSPF Multipoint Relay (MPR) Extension for Ad-hoc networks etc. The mentioned protocol does not provide any type of securities; the malicious node can easily participate in routing operation. To overcome the security problems other secure routing protocols can be found in MANET. The secure protocols add the security functionality to existing routing protocol for the purpose of secure routing protocol in [4]. In the secure routing, two types of technique can be introduced in these protocols: Assuring Authentication and Integrity of routing messages, both techniques allow nodes to monitor the behavior of other nodes in routing operation.

In this paper, we’ll discuss our implementation of the AODV protocol extension in brief.

2. AODV
AODV [5, 6] which stand for Ad-Hoc on demand distance vector is one of the well known reactive routing protocol under the MANET networks. As its name reflects it facilitates route discovery on-demand. Nodes in the AODV network exchange information through routing table, here a route is established between the source and receiver, between whom communication takes place through routing process. AODV is capable of both unicast and multicasting routing. It is loop free, self-starting and scales of large number of mobile nodes.

In the AODV, when one of the node which act as a source node, want to send data packet to some destination node, so it first check out a route table to find out whether it has route or not. If the route exist that route can be used for the transmission of data and if not, so in that case another mechanism has started (i.e. a Route Discovery Process). This route discovery process began through sending RREQ (Route Request Process). Nodes receiving this packet update their information for the source node and set up backwards vector to the source node in the route tables. The RREQ contain the source node IP address, current sequence number. Broadcast ID and the most recent sequence number for the destination of which the source node is aware.

As the RREP packet propagates back to the source, nodes set up the forward vector to the destination. Once the source node receive the RREP packet, it may be to forward the data packet to the destination. If the source node receive a RREP packet in delay the packet containing a greater sequence number or contain the same sequence no. (AODV uses sequence no. to ensure the freshness of routes) with a smaller hop-count, it may update its routing information or update the routing table for that destination and used the update and better route. As long as the route the route remains active, it will necessary to maintain the route. A route is active to source to destination and the data packet periodically travelling from along the path. If the source node stops sending data packet the link will time out and route entry deleted from the intermediate node routing table. If the link break occurs while the route is active, the neighbor node upstream of the break propagates a route error (RERR) message to the source node to inform that the destination node now unreachable. After receiving the RERR, if the source node still wants the route, it can reinititate route discovery.
AODV does not give the complete view of topology to the nodes each node react a neighbor and non-neighbor nodes. It knows only the next-hop to reach them and the distance.

3. MNAP (Malicious Node Attack preventer) Approach
MNAP is an AODV protocol extension, which uses the Pre-Key Distribution or pre deployed key’s Approach with the use of reserved field in RREQ & RREP packet [5] respectively. The many type of pre-key distribution approaches [7, 8, 9, 10, 11] used in the ad-hoc network for security perspectives. The pre key distribution approach facilitate that, the node should have the knowledge of all deployed key’s information in the network. In MNAP we used the simple and effective pre-key distribution approach.

In AODV, the reserved field of RREQ and RREP packet header always zero (0) or it is not used. The nodes are not check or processed the reserved field information while ignored on reception.

In MANP we have made changes in the request and reply phase of the AODV, where 11 reserved bits were available in request phase and 9 bit ware available in reply phase to us. The mechanism of MNAP divided in three parts: Matrix Creation, key Selection, and Bit Operation.

3.1 Matrix Creation
In matrix creation, first a matrix is formed in the form of (X, Y). Where X represent column and Y represent row. The total no of element in the matrix is defined as,

\[ [x][y] = 2^{\text{no.of reserved bit in RREQ packet}} \]  
\[ [x][y] = 2^{\text{no.of reserved bit in RREP packet}} \]  

The formation of the matrix generation is,

\[
\begin{bmatrix}
  x_1 & x_2 & x_3 & \cdots & x_n \\
  y_1 & a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\
  y_2 & a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\
  y_3 & a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\
  \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  y_n & a_{1n} & a_{2n} & a_{3n} & \cdots & a_{nn}
\end{bmatrix}
\]

If repetition of matrix value (key) is allowed then there is no limitation on the matrix. For RREQ, \(2^{11}\) give 2048, \(2^8\) give 512 and the permutation and combination of these number is very large hence we can use the large number of keys in the network.

3.2 Key Selection
After the matrix creation, we select the bit (element) from the matrix for RREQ and RREP. The key selection mechanism uses the different field’s information of the RREQ and RREP packet.

The Mechanism of bit selection is:-

For RREQ

\[ X = (\text{Source seq.no.} \cdot z) + (\text{Hop Count} \cdot z) \]  
\[ Y = (\text{Dest. IP add} \cdot \text{z}) + (\text{Dest. Seq.no.} \cdot z) \]  

For RREP

\[ X = (\text{Dest. IP add} \cdot z) + (\text{Hop Count} \cdot z) \]  
\[ Y= (\text{Dest. Seq.no.} \cdot z) + (\text{Dest. IP add} \cdot z) \]  

Where \((z) = \text{order of the matrix}\).

Finally, uses this given equation we calculate the value \(Y\) (row) & \(X\) (column) after calculation where \(X\) & \(Y\) intersect in the matrix then the key will be select. In the above equation the reason of uses different field information (Hop Count, Source & Destination Seq. No) of the packet provide the efficient and different keys selection because after every hop a packet of information is changed.

3.3 Bit Operation
In bit operation, selected bit convert into the binary and place in reserved field in RREQ and RREP packet header and propagate in the network. In given matrix the bit selector selects the bit (see highlights bit) for RREQ & RREP. The all matrix element (in binary) also define in the network.

\[
\begin{bmatrix}
  x_1 & x_2 & x_3 & \cdots & x_n \\
  y_1 & a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\
  y_2 & a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\
  y_3 & a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\
  \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  y_n & a_{1n} & a_{2n} & a_{3n} & \cdots & a_{nn}
\end{bmatrix}
\]

For RREQ For RREP

Hence the all keys in the form hexadecimal (0X0000FF00). The key include the all packet header information as well as matrix selected value (key).

For example; we create a \([x, y] = [5^45]\) matrix the total number of the element in this matrix = 25. Total element of the generated matrix value lies in 1 to 25 and order of the matrix = 5. After the matrix creation, the same matrix uses in both packets, and select the keys by the help of key selector in given matrix.Suppose 17 (RREQ) and 20 (RREP) key are selected then the selected key converts in to the binary and placed in reserved field in RREQ & RREP packet header.

4. Attacking AODV and MNAP
AODV doesn’t provide any type of security. AODV messages are not generally encrypted, authenticated, or integrity protected and basically always assumed as trusted. Many types of attacks are possible a systematic analysis of AODV security is proposed in [12, 13]. For testing the AODV and MNAP in simulation scenario we create a one parameter i.e. by creating trustworthy and Non-trustworthy node in the network by putting two values: 1= trustworthy node and 0 = non-trustworthy node. The trustworthy nodes have the knowledge of the keys information& keys selection and non-trustworthy nodes doesn’t have the knowledge of the key, resulting this, thus non-trustworthy node drops the all data packets. And two type of attack in the network: Gray-Hole [14] and Black-Hole [15].

Gray-Hole: An attacker forwards all RREQs and RREPs but forwards only a few data packets, dropping all other data packets. Clearly it points out a lapse in the routing protocol. This type of attack is known as gray-hole problem.
Black-Hole: An attacker can project itself as having shortest route to a destination. The attacker also can generate false error message and spreading fake information in the network.

Firstly, we developed a block-hole attack in the network. It knows of the ways of duping the source node about the route to the destination by sending a RREP as an intermediate node to the destination, telling it that it has a very good route to destination node with high sequence number, lifetime and very good hop count. This makes the source node feel that it can never find a route better than this and thus starts sending all the data to this Non-trustworthy node. The attack is shown in fig 1.1. Dashed lines represent direct radio visibility, solid line represent data traffic. Before the attack in AODV, node A sends a RREQ for node F, and node F replies. Thus the route is established between nodes A and F, with traffic following through intermediate node D.

![Before the Attack in AODV](image1)

![During the Attack in AODV](image2)

then due to mobility the non-trustworthy node M take the position of node D. when the non-trustworthy node (M) wants to being its attack, it first must establish its own route towards node A and F using propagate fake RREP message. Sending the fake RREQ messages, node M easily established the route between node A and F but creating a packet dropping effect, node M drop all data packets. And this cause, packet dropping effect and Black-Hole attack AODV resulting 0 (zero) PDR (packet delivery ratio). Or in other words, AODV not worked.

Secondly we create a Gray-Hole attack in the network. In this type of attack, the attacker forwards few data packet to destination. Now it is the courtesy of the attacking node to decide about what to do with the information in the packet whether to drop all, or let some pass. To avoid this kind of attack AODV does nothing resulting in very less PDR.

In MNAP, during the attack (Black-Hole & Gray-Hole) the attacking node not initiate in the network because they don’t have the information about keys and keys selection. In the Fig 1.1 during the attack, based on the key received a node can decide whether to accept the RREP & RREQ and process it or directly drop it resulting in expelling a non-trustworthy node M (malicious node) out of the route with no chance to it available it to be part of the route resulting in a better PDR and throughput for this modified approach.

5. Simulation and Result
In order to analyze and compare the performance of the two routing protocols AODV and MNAP simulation experiment were performed with the Random Way-Point Mobility Model [16]. The following Random way-point parameter has shown in Table 1.1 Position granularity is used for Qualnet network simulator to calculate the frequency of updating the position of each node.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Speed</td>
<td>0 mps</td>
</tr>
<tr>
<td>Maximum Speed</td>
<td>10 mps</td>
</tr>
<tr>
<td>Pause Time</td>
<td>30 second</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250 meters</td>
</tr>
<tr>
<td>Position Granularity</td>
<td>1.0 meter</td>
</tr>
</tbody>
</table>

Table 1.1

Traffic sources used was CBR (Constant Bit Rate). The packet size was 512 bytes and item to send 100 (total 29 CBR packets) and set the stat time in 1 sec and end time 100 sec in
total simulation. For all experiments, the IEEE 802.11 MAC layer protocol was used.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>200 seconds</td>
</tr>
<tr>
<td>Scenario 1</td>
<td>50 nodes, 3 CBR source, 1.5 km² field</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>100 nodes, 3 CBR source, 1.5 km² field</td>
</tr>
<tr>
<td>Scenario 3</td>
<td>150 nodes, 3 CBR source, 1.5 km² field</td>
</tr>
<tr>
<td>Scenario 4</td>
<td>200 nodes, 3 CBR source, 1.5 km² field</td>
</tr>
<tr>
<td>Non-trustworthy Node</td>
<td>12-15% in each scenario</td>
</tr>
</tbody>
</table>

Table 1.2

In table 1.2, to evaluate the parameter and protocol in different scenarios with many nodes, we ran simulation tests using the Qualnet Network Simulator [17]. Attention has been focused on four performance metrics.

5.1 Packet delivery ratio

It is the ratio of the number of delivered data packet to source to destination. In Fig 1.2 gives the experimental view of packet delivery ratio.

5.2 End-to-End delay

End-to-End delay indicates the average time taken by a data packet CBR (constant bit rate) to arrive at the destination. It also includes the delay caused by route discovery process. It may be seen from Fig 1.3 AODV takes too much time for establish the route and packet sending.

5.3 Throughput

It is the average rate of successful message delivery over a communication channel. In other words, throughput is the number of bits that can pass through the medium (wires) in one second. It is clear from Fig 1.4 the MNAP gives the better throughput against AODV.
5.4 Packet drop by non-trustworthy node
Packet drop by non-trustworthy node indicates the average packet dropping effect. In Fig 1.5, AODV mostly drop the all data packet. We test the both protocol with 3 CBR applications if we increase the CBR in each scenario then, the packet dropping effect also increases.

![Fig 1.5](image_url)

6. Conclusion
In this paper, MNAP was presented, an extension implementation of the AODV routing protocol. MNAP adds security to AODV but includes keys information and keys selection operations that can have a significant impact on performance. We discuss the how we add the information in reserved field of RREQ and RREP packet and how we process and check it. Other possible improvements could be added for example, Non-trustworthy node creation (which seems to have positive impact on performance). However AODV performed poorly for most of the matrix (PDR, Throughput). While MNAP increase the ratio of performance in all matrix. The implementation of the protocol has been done using C++ language.

7. References


[17] Qualnet Simulator