Optimized & Secure Ad-hoc on Demand Distance Vector Routing Protocol

Praveen Lalwani¹, Piyush Kumar Shukla¹

¹CSE Department, University Institute of Technology, RGPV, Bhopal
praveen.lalwani@gmail.com, pphdw@yahoo.com

Abstract A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes in which different routing protocols are used to form the communication network. So, far there are numerous routing protocols are discovered in which AODV performs superior than all. Ad-hoc network suffer from the bunch of issues in which congestion and security are the major issues of concern which leads to severe degradation of network throughput and Packet Delivery Ratio. It also increases the routing overheads and end to end delay. This paper presents a novel design Optimized and Secure AODV which is the modified version Optimized AODV by including new Packet Route Checker. The Route Checker Packet is the additional mechanism in the Optimized AODV to create obstacle against Black-hole attack. The result shows that OSAODV performs better in terms of Packet Delivery Ratio and Throughput than AODV. The simulation has done through network simulator NS-2.

Keywords: Routing, Malicious, AODV, Black-hole

1 Introduction

1.1 Routing

Routing is the process of transmitting information from a source to destination. For wired networks the two main routing algorithms used First, Distance Vector Routing. Second, link State Routing. A distance vector routing algorithm is a distributed algorithm that is simple to develop and has low comprehend demands. It means that each router has a way of knowing about its neighbors.

Instead of depending on every neighbor to regularly give information about how to get to all the destinations the link state routing algorithm gets a complete picture of the whole network and locally calculates the shortest path from source to every destination.

© Elsevier, 2012
1.2 Routing in Ad-hoc Networks

In the case of a mobile ad hoc network, topology is changing dynamically. This leads to rapidly changing link states. Some links to get broken while other links are created by other pairs of routers at the same time. The ad-hoc network is a collection of communication devices or mobile devices (nodes) which communicate with each other through wireless medium without any centralized or fixed infrastructure. The nodes in ad hoc networks can be stationary or mobile. In the absence of the centralized infrastructure implies that the accountability of the nodes is equal. Therefore, participating nodes in the network need to co-operate in order to establish routes and to forward packets for other nodes. The nodes use routing protocols to establish and maintain the routes. The commonly used standard for ad hoc networks is IEEE802.11b (Wi-Fi), which is the standard for WLAN.

1.3 AODV

In AODV [1], the network [2] is silent until a communication is needed. At that point when any network node [3] wants to send the data to another node it needs to broadcast a route request packet for a new connection [5]. Other AODV nodes forward this message, and when the route request message received at Target node then it replies by Route Reply packet. After the route establishment, communication takes place between the sender and receiver. If any of the link failure occurs in the communication path then the Route Error packet is sent back to the transmitting source. Unused entries in the routing tables are recycled after a time and the process repeats.

1.4 Black-Hole Attack

The Black-Hole attack has two properties [6]. In First one, the node vanishes the mobile ad-hoc routing protocol, such as AODV, to present itself as having a legal route from source to a destination node, even though the route is fake, with the intention of capturing packets. The second one, the attacker consumes the captured packets without any forwarding [7]. There is a more intelligent form of these attacks when an attacker selectively forwards packets. An attacker suppresses or changes packets originating from some nodes, while leaving the data from the other nodes unaffected.

2 Proposed Concept

Optimized and Secure AODV is the modified version of Optimized AODV [1] as shown in fig 1.1 in which one more parameter is added is security. Initially Route Request packet broadcasts on the network to establish the new path for the communication and when packet received at the destination it reply by unicasting the Route Reply Packet RREP. If the path break-up there then optimized AODV is used.
to recover the new path as shown in figure 1.2 and for security purpose route checker packet added into it as shown in fig 1.3.

Optimized AODV is modified version of ELRAODV [2] which uses next to the next node to recover the path. If the route is not repaired by ELRAODV (Enhance Local Repair AODV) then instead of sending RRER packet it sends PRRER (priority route error packet) which is the extension of RRER packet to set the priority of the packet [1]. If some packet is waiting in the queue to be forwarded then instead of forwarding these packets, forwards the priority packet is first. If this PRRER packet reaches with shorter delay to the source it stop sending extra packets in the network which
decreases routing overhead and end to end delay. It also increases throughput and packet delivery ratio.

2.2 Detection of Malicious Node

The route Checker packet is added to the Optimized Aodv as shown in fig 1.3. We have stored next to the next node address in the routing table, this address used in the Route checker packet and two bits is used for acknowledgment bit ‘1’ shows true and a bit ‘0’ show fails. In the communication after 5 ms second each and every node send route checker packet to the next to the next node and a route checker packet receiving node checks that the data packets received from the previous node or not, then it sends the acknowledgment to the route checket packet sender by bits ‘0’ or ‘1’. Bit value ‘1’ acknowledged to the sender, if data packets received from the previous node and it represent previous node is trustworthy or next node from the sender is trustworthy. If it does not receive the data packets from the previous node then bit ‘0’ is acknowledged by the help of which receiver node know the next node is black hole or malicious because the property of the black hole node it drops the packet instead of forwarding it.

![Fig 1.4 Black-Hole Detection](image)

As shown in the figure 1.4 each and every node send route checker packet to next to next node node 1 send the route checker packet to node 3 it is replied by bit 1 means node 2 is trustworthy other and node 3 send the route checker packet to node 5 it replied by bit 0 means node 4 is malicious or Black-hole node.

3 Simulation and Analysis

Simulation has been done using 10, 20, 30, 40 and 50 Nodes [8]. There are four parameters, end-to-end delay, routing overhead, packet delivery ratio and throughput have been analyzed, which are directly related to congestion. The end-to-end Delay and routing overhead get increased (i.e. As shown in the Table 1) due to the extra packet needed to check whether any node is malicious or not? If the node is found to be malicious then it can be removed from the network and new path establish for the communication with the help of RREQ routing [2] packet. Packet Delivery Ratio and
throughput gets increased as shown in the Table 1, when the malicious node is detected and removed from the network, as we know that the property of the black hole node is to drop the packets. Graph of experimental result shown in the fig 1.5, fig 1.6., 1.7 and 1.8 has been generated using a simulation through standard network simulator i.e. NS-2.34.

**Table 1**: Comparison of OSAODV with AODV on the basis of different Key Performance Parameters where RO: Routing Overhead, EtE: End to End Delay, PDR: Packet Delivery Ratio

<table>
<thead>
<tr>
<th>AODV (Nodes)</th>
<th>RO</th>
<th>EtE</th>
<th>PDR</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.004</td>
<td>15.1676</td>
<td>0.126473</td>
<td>47.11</td>
</tr>
<tr>
<td>20</td>
<td>0.029</td>
<td>503.846404</td>
<td>0.128959</td>
<td>188.54</td>
</tr>
<tr>
<td>30</td>
<td>0.027</td>
<td>767.359753</td>
<td>0.003833</td>
<td>8.05</td>
</tr>
<tr>
<td>40</td>
<td>0.025</td>
<td>796.408284</td>
<td>0.010109</td>
<td>162.59</td>
</tr>
<tr>
<td>50</td>
<td>0.121</td>
<td>669.228105</td>
<td>0.010400</td>
<td>169.11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OSAODV (Nodes)</th>
<th>RO</th>
<th>EtE</th>
<th>PDR</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.004</td>
<td>686.413282</td>
<td>0.110073</td>
<td>65.56</td>
</tr>
<tr>
<td>20</td>
<td>0.029</td>
<td>665.441734</td>
<td>0.144211</td>
<td>282.56</td>
</tr>
<tr>
<td>30</td>
<td>0.030</td>
<td>869.335491</td>
<td>0.003033</td>
<td>19.11</td>
</tr>
<tr>
<td>40</td>
<td>0.099</td>
<td>804.425840</td>
<td>0.008910</td>
<td>181.53</td>
</tr>
<tr>
<td>50</td>
<td>0.089</td>
<td>629.789828</td>
<td>0.010404</td>
<td>169.11</td>
</tr>
</tbody>
</table>

**Fig 1.5** End to End Delay  
**Fig 1.6** Packet Delivery Ratio  
**Fig 1.7** Routing Overhead  
**Fig 1.8** Throughput
4 Conclusion and Future Research Direction

In this paper Optimized and Secure AODV has been simulated, results as shown in Fig.1.6 and Fig.1.4 clearly shows that as the number of nodes increase routing overhead around 24 % and end to end delay Increases around 32% in OSAODV as compared to the AODV. Due to lower routing overhead of OSAODV network performance improved. The results shown in Fig 1.7 and Fig. 1.5 indicate as the number of nodes increase throughput and Packet delivery ratio increases by 25 % in OSAODV as compared to the AODV.

The proposed solution is, in most cases, not tested in a real environment Therefore, future studies should rather be devoted to real implementation than just a simulation and to develop prevention against different kinds of attack like gray hole which is an advance version of the Black Hole attack. Only such an approach can ultimately verify a protocol’s usefulness in future ad-hoc and other mobile networks.

References