Pre-Path and Post-Path Security to Mobile Adhoc Network
Zalte S. S.*,1, V. R. Ghorpade2
1Computer Science, Shivaji University, Kolhapur, Maharashtra, India
2D.Y.Patil college of Engineering, Shivaji University, Kolhapur, Maharashtra, India

ABSTRACT

This paper represents secure AODV protocol for Mobile Adhoc Network (MANET) with the objective that each data packet must be securely reached to the destination. To achieve this objective, we have divided work into two parts, pre-path security and post-path security. In pre-path security we have used secure neighbor discovery. In post-path security we have used hybrid cryptography. The proposed secure AODV protocol aims to provide security to path and data packets. After modifying AODV protocol we get marginally increased packet count, Packet Delivery Ratio and throughput.

Keywords: AODV, MANET, secure neighbor discovery, security to path, Hybrid cryptography.

I. INTRODUCTION

In Mobile Adhoc Network (MANET), data operations are not suffered from passive attacks such as eavesdropping, traffic analysis, monitoring etc[1]. Here we have used cryptography to prevent passive attacks. Internal attacks are more dangerous than passive attacks as shown in Table1. They are fired from compromised nodes. These types of attacks disturb routine functions of system in order to consume energy, memory and other resources. Internal attacks such as fabrication, interruption, interception and modification. These types of attacks are very difficult to differentiate between normal activities and malicious activities of network. Cryptographic graphical security primitives such as integrity, authentication, confidentiality and non-repudiation used to combat against external attacks not against internal attacks if it get compromised and get secret information from other nodes. For that there is highly requirement of Intrusion Detection System to combat internal attacks. So we have also used IDS to detect and prevent some attacks like ddos, replay, black hole.

Routing is most imperative task in Mobile Adhoc Network. To develop up routing protocol for this type of resource constraint network, in terms of memory, energy, battery. Because of its unique characteristics like imprudent structure, dynamic topology, asymmetric links etc. to develop routing protocol is quite challenging job. The improper or insecure design of routing protocol leads deteriorated performance of network. Such network render more prone to various attacks.

II. LITERATURE REVIEW

In paper [2] author have proposed aodv-sec protocol which is extension to saodv protocol. Public key infrastructure and X.509 certificate used as trust anchor for node identification. But due to cryptographic primitives this scheme is not suitable for large network.

A author have secured on demand routing protocol in paper[3], Dynamic Source Routing. In this protocol not only source and destination but also intermediate nodes are authenticated. The main task of this protocol to allow intermediate nodes to authenticate its predecessor node and also detect attacks like modification, fabrication and fake req. Finally destination node authenticate all nodes in the route. This protocol provides security against reply attack, rushing attack, IP spoofing and man in the middle attack. Protocol is based on asymmetric cryptography, so it consumes more battery due to lot of calculation.

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Hack Pack</th>
<th>View</th>
<th>Modifying Data</th>
<th>Modifying Protocol Data</th>
<th>Change Node Behavior</th>
<th>Change Network Behavior</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

Table1.
To improve performance and security, the author proposed the AODV protocol in [4]. The security of AODV will be based on one-way hash, two-way hash, and digital signature. Here, the author generates two signatures. Intermediate nodes verify only the first signature and accept the packet, and the destination node verifies the second signature to check authenticity and integrity. Advantages of this scheme are no certificate and key management scheme, less overhead of calculation, and less battery consumption.

A author has proposed a mechanism that provides Secure Route Discovery for the AODV protocol (SRD-AODV) in order to prevent black hole attacks in [5]. This mechanism requires the source node and the destination node to verify the sequence numbers in the Route Request (RREQ) and Route Reply (RREP) messages, respectively, based on defined thresholds before establishing a connection with a destination node for sending the data.

In paper [6], the author has proposed trust-based secure routing protocol (TSDRP). This proposed Framework Architecture mainly has three modules (i) Direct Observation (ii) Promiscuous Mode Observation and (iii) Trust Module for Secure Route Discovery Establishment, its Maintenance and Attack Prevention. TSDRP is designed to prevent malicious actions like Black hole attack and DoS attack by calculating trust value for their neighbours based on the proposed framework.

STAND is proposed in [7] which is applicable for both scenarios static and mobile to detect worm hole attack and also detects nodes which are affected by worm hole attack. The author divides nodes into two groups: correct and incorrect neighbours. IT locates one node at the centre and neighbours of centre nodes are considered as correct neighbours and relaying other nodes considered as incorrect nodes. The author has used a 3D graph which fits all nodes, correct nodes should have a smaller distance, and incorrect nodes should far away. Computational cost of STAND is less than MSDN. STAND has lower computational complexity than other protocols. This protocol is robust to ranging error and has a high accuracy. The computational complexity of this protocol is lower.

Without compromising Quality Of Service, the author has provided security in [8] by analysing the behaviour of nodes selfishness and malicious. The protocol constructs trusted path by excluding malicious and selfish nodes. Security is deployed by using public key cryptography between sender and receiver. In case of multi-path visual cryptography is applied on data and equally on path.

### III. PROPOSED WORK

The secure AODV protocol aims to provide security to path and data packets. A AODV protocol combines feature of DSR and DSDV routing protocol. In AODV routing process, hop by hop routing is same like DSDV protocol and route discovery process same as DSR. It differs with DSR in the way that it does not store the information of entire route in its buffer. And Route maintenance is same as DSDV[9]. Pure reactive routing protocols like AODV and DSR more suitable for large adhoc networks and topology is dynamic[10].

This solution composed in four stages as shown in Fig.1.

**Secure Neighbour Discovery:** Having the legitimate nodes is one of the most prominent features in secure routing protocols. When data routes in network it reached destination only from the secured hand.

- **a)** One hop authentication: Here each node determines first-hop neighbours by sending hello packets with its ID (here we consider public key as node id) After receiving hello packet. Receiver node send reply packet which contains nonce which is authenticated by itself one by one by sending hash value of nonce. Initiating nodes accepts only those reply packets which are received within time stamp. It adds into their expected neighbour list. This list may contain some nodes which are not within initiators communication range but due to malicious node which relay hello and reply packets to these nodes.

- **b)** Two hop authentication: Once expected neighbour list received then in two hop neighbours. We have search neighbours of each node in this expected neighbour list. Here each node use receivers public key to encrypt the expected neighbour list and list of hash values of nonce which are used in searching first hop neighbours. Each node broadcast encrypted expected neighbour list. Each node waits reply for neighbours of expected neighbour list within timestamp.

**Secure and Efficient Nodes Selection:**

Node selection process runs parallel. In this process nodes which are detected maliciously in neighbour discovery process and which are detected at network layer are ignored and The nodes which are legitimate having adequate are selected.
Forward Data Packets with Cryptographic Shield:-
We have used hybrid cryptography in providing security to data packets. In this phase we have used combination of symmetric and asymmetric cryptography in order to achieve security primitives like integrity, authentication, non-repudiation and confidentiality.

Parallel Run Intrusion Detection System:- For the second line of defence we have used defence mechanism against routing attacks such as Distributed Denial of service, replay, modification, fabrication etc. In proposed protocol three attacks are detected Distributed Denial of service, replay and black hole. If attackers impose these attacks then for some time attackers are banned for network transmission. After some time they may get chance to participate in network and to transmit data packets legitimately.

In this proposed protocol neighbour discovery protocol runs after one second, so node detection will be done constantly.

IV. RESULTS

We have simulated and compared proposed protocol with original using network simulator tool (NS3). Table 2 shows simulation parameters. Simulation result shows that modified secure AODV routing protocol marginally increases packet delivery ratio, throughput and packet count better than the old AODV.

For result analysis, we have considered some of the parameters like packet delivery ratio(PDR), throughput and packet count with a set of number of nodes which vary from 25,50,75 and 100. These parameters are compared with old AODV and proposed modified secure AODV protocol. So we able to evaluate the performance of the proposed secure AODV protocol. Green line shows graph of proposed secure AODV protocol and red line shows graph of normal old AODV protocol.

Table 2: Simulation Parameters(NS3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes</td>
<td>25, 50, 75, 100</td>
</tr>
<tr>
<td>Area Size</td>
<td>500 X 500</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>20 sec</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512</td>
</tr>
<tr>
<td>Protocol</td>
<td>AODV</td>
</tr>
</tbody>
</table>

In Figure 2. depicted graph of number of nodes vs. packet count. Figure 3. depicted graph of number of nodes vs. throughput and in Figure 4. depicted graph of number of nodes vs. packet delivery ratio. These Figures shows that proposed secured AODV protocol raised packet count, throughput and packet delivery ratio marginally.

![Figure 1: Proposed Secure AODV Protocol](image)

![Figure 2: Node vs. Packet Count](image)

![Figure 3: Node vs. Throughput](image)

![Figure 4: Node vs. Packet Delivery Ratio](image)
V. CONCLUSION

In MANET there are no bindings or restrictions on the participation of nodes in the network. Data transmission is extremely dependent on the cooperation of participant nodes. This makes manet more prone to variety of different attacks. That's why in this proposed protocol, we have to decided to provide security before routing starts that is pre-path security and during routing that is post-path security. In this process, first we have detected and removed malicious nodes from routing path and then we have provided data packet security by using hybrid cryptography. Modified secure AODV protocol get satisfied results over the old AODV protocol in terms of throughput, packet delivery ratio and packet count.

VI. REFERENCES


