CHAPTER 5

CRYPTOGRAPHIC SOLUTION

One of the biggest challenges when it comes to secure the mobile AdHoc network is all of the factors that must be accounted for: dynamic topologies, resource constraints, lack of infrastructure and limited physical security. Evidently, knowledge about cryptography and its special customization with MANET will provide the research community with the latest updates in cryptographic techniques and bring new perspective to security, performance, and many other areas of high importance in MANETs. The focus of cryptography and its basic applications in MANETs will build the foundation for advanced research in security (Chen and Wu 2012).

In MANET, two types of messages are used. They are data messages and routing or control messages. Data messages need end to end authentication and can be secured using point to point security mechanism. Routing messages are used for the route establishment and route maintenance. Routing messages are processed by intermediate nodes during their propagation therefore securing routing messages is more challenging compared to data messages. Routing protocols must be robust against routing attack in order to establish correct and efficient route between pair of nodes.

This chapter proposes two cryptographically based routing protocols Two Tier Secure AODV (TTSAODV) and Two Tier Secure AOMDV (TTSAOMDV). In literature, most of the available solutions against black hole attack are based on the sequence number in the RREP. As
an attacker, the black hole node may change the sequence number slightly higher than the original which cannot be identified by the source node. So, the mitigation technique based on the comparison with sequence number will not be efficient. The solution must be included with some verification techniques during the route discovery process. Thus, the proposed protocol TTSAODV and TTSAOMDV identify single as well as collaborative black hole attack by verifying the trueness of the RREP message with Verification messages sent by neighbours of the intermediate node which sent the RREP without considering the sequence number in the RREP. The basic assumption in this solution is that there is a strong symmetric key distribution system in the MANET. Thus, every pair of nodes in the network has unique common secret key.

Three additional modules have been included with the conventional AODV and in AOMDV.

1. Authenticated Route Request and Route Reply
2. Tier 1 security – Verification by neighbour nodes
3. Tier 2 security – Verification with control messages

Even if the detection of black hole attack fails at tier 1, in tier 2, it will be identified definitely. So, the proposed protocol has high degree of attack detection and prevention.

5.1 MESSAGE FORMATS IN AODV

In AODV, a node disseminates a RREQ when it determines that it needs a route to a particular destination and does not have one available. This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination expires or is marked as invalid. The Destination Sequence Number field in the RREQ message is the last known
destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. The message formats of RREQ and RREP of conventional AODV is shown in Figures 5.1 and 5.2 respectively.

<table>
<thead>
<tr>
<th>Type</th>
<th>Reserved (11 Bits)</th>
<th>Hop Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RREQ ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Sequence Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Originator IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Originator Sequence Number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5.1 RREQ Message Format**

<table>
<thead>
<tr>
<th>Type</th>
<th>Reserved</th>
<th>Prefix</th>
<th>Hop Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Sequence Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Originator IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life Time</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5.2 RREP Message Format**

In AODV and AOMDV routing protocols, routing messages RREQ or RREP have two types of information: Mutable and Non Mutable. The hop count is only mutable field as intermediate nodes increment the hop count field while forwarding the RREQ. The rest fields such as sequence number or IP address are non mutable fields as they remain unchanged.

The proposed protocol modifies the RREQ and RREP of the conventional AODV with authentication in order to secure the authenticity of
non mutable fields in the routing messages. Thus modification either in sequence number or in IP address by any intermediate node will be avoided, and hence the attacks like modifying routing information and impersonation can be avoided.

5.2 AUTHENTICATED ROUTE REQUEST IN TTSAODV

In the proposed two tier secure AODV, the source node S initiates the route discovery by broadcasting RREQ as follows:

\[ S \rightarrow AD_S|ID_{RREQ}|Seq_S|AD_D|Seq_D|HC|N_S|MAC(K_{SD}|AD_S|ID_{RREQ}|Seq_S|AD_D|Seq_D|HC|N_S) \]

Here, AD_S and AD_D denote the IP address of source node and that of destination node, ID_{RREQ} is the broadcast ID, Seq_S and Seq_D represent the sequence numbers of source and destination node, HC is the number of nodes this message has passed and N_S is a nonce (random number) generated by the source. Here K_{SD} is the common secret key of Source node and the Destination node. Here the MAC algorithm used is a modified Secure Hash Algorithm 1 (SHA1). The modified RREQ message format is shown in Figure 5.3

| Type   | Nonce (1 Byte) [N_S] | Modified Hash (10 bites) [MAC(K_{SD}|AD_S|ID_{RREQ}|Seq_S|AD_D|Seq_D|HC|N_S)] | Hop Count [HC] |
|--------|---------------------|-----------------------------------------------------------------|----------------|
| RREQ ID | [ID_{RREQ}]         | Destination IP Address [AD_D]                                   |                 |
|        |                     | Destination Sequence Number [Seq_D]                            |                 |
|        |                     | Originator IP Address [AD_S]                                    |                 |
|        |                     | Originator Sequence Number [Seq_S]                             |                 |

**Figure 5.3 Modified RREQ Message Format**
5.2.1 Modified SHA1 Algorithm

The conventional SHA1 algorithm produces 160 bits of hash value. Since, the proposed routing protocol aims to enhance the conventional AODV without modifying the structure of AODV and without much routing message overhead, the reserved field of 11 bits available in the RREQ message is used for authentication. In the available 11 bites, only 10 bites are allotted for sending the hash value. So, in order to use the available 10 bytes and to preserve the originality in complexity of SHA1, the algorithm is modified. Figure 5.4 shows the block diagram of modified SHA1.

The message to be authenticated, for example, in RREQ, the message $AD_S|ID_{RREQ}|Seq_S|AD_D|Seq_D|HC|N_S$, is applied to the conventional SHA1 algorithm with secret key shared by the source and the destination. The SHA1 produces 160 bit hash code. Then, this hash code is split into 16 words of 8 bits each. And these sixteen words are applied to an 8 bit EXOR operation. As a result, an 8 bit modified hash code will be produced.

![Figure 5.4 Block Diagram of Modified SHA1](image)

5.3 PROCESSING OF RREQ

When any intermediate node receives the RREQ, it checks whether the destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the Destination Sequence.
Number of the RREQ. If so, the route in the intermediate node is considered as the fresh enough routes. Based on the availability of the fresh enough route, two cases will be considered.

5.3.1 Case 1 – Non-availability of Fresh Enough Route

The intermediate node (AD$_I$) which has no route to the destination node would add the hop count field HC by 1 (HC$_n$), rebroadcast this RREQ to its neighbours and sets up a Reverse Path Pointer for the node from which it receives the RREQ. The rebroadcasted message will be of the form:

$I\rightarrow AD_I|AD_S|ID_{RREQ}|AD_D|Seq_D|HCn|N_S|MAC(K_{SD}, AD_S)|ID_{RREQ}|Seq_S|AD_D|Seq_D|HC|N_S$

5.3.2 Case 2 – Availability of Fresh Enough Route

When the intermediate node has the fresh enough route, it generates RREP to the source node S. When generating a RREP message, a node copies the Destination IP Address and the Originator Sequence Number from the RREQ message into the corresponding fields in the RREP message. Processing is slightly different, depending on whether the node is itself the requested destination or instead it is an intermediate node with a fresh enough route to the destination. Again, two cases are considered.

5.3.2.1 Case A – RREP by an Intermediate Node

The intermediate node, which has the fresh enough route copies its known sequence number for the destination into the Destination Sequence Number field Seq$_UD$ in the RREP message. And it updates the forward route entry by placing the last hop node (from which it received the RREQ, as indicated by the source IP address field in the IP header) into the precursor list for the forward route entry, that is, the entry for the Destination IP Address. The intermediate node also updates its route table entry for the node
originating the RREQ by placing the next hop towards the destination in the precursor list for the reverse route entry, that is, the entry for the Originator IP Address field of the RREQ message data.

The intermediate node places its distance in hops from the destination (indicated by the hop count in the routing table) Count field $HC_U$ in the RREP. The Lifetime field LT of the RREP is calculated by subtracting the current time from the expiration time in its route table entry.

The format of RREP packet generated by the intermediate node is as follows:

$I_R \rightarrow AD_P|AD_N|AD_{DS}|AD_{D}\|Seq_{RD}|HC_{U}\|N_{S}|LT|MAC(K_{SDS}|AD_{S}|ID_{RREQ}|Seq_{S}|AD_{D}|Seq_{D}|HC_{N_{S}})$

In this, $AD_P$ denotes the IP address of the previous node of the Intermediate node towards source node and $AD_N$ denotes the IP address of the next node to the destination. This intermediate node may be a malicious node, which can modify the IP address. But this can be verified at the source using MAC. Thus impersonation attack can be avoided. But in the case of black hole attack, the sequence number in the RREP message can be modified with a higher number than the original. Also, if the increase in forged sequence number is very less, it may not be identified by the source with the previous proposal, since in previous proposal, only when the increase in sequence number is higher than the threshold, the RREP is assumed from a malicious node. An intelligent malicious node may predict the dynamic threshold updation and it can increase the sequence number in such a way that, it cannot be identified by the threshold comparison. Thus, there must be some other provision to verify the authenticity of route through this intermediate node. In this proposal, this authenticity is provided by Tier 1.
5.3.2.2 Case B - RREP by Destination

When the destination node receives the RREQ, it accepts the RREQ with the valid MAC, which first reaches it. If the sequence number is bigger than the same route stored in its routing table, it updates the routing table to store $AD_s$, $ID_{RREQ}$ and the sequence number. Finally it sends the RREP to the source node.

The format of RREP packet generated by the destination is as follows:

$$DR \rightarrow AD_s|AD_d|Seq_{UB}|N_d|LT| MAC(K_{SD}, AD_s|AD_d|Seq_{UB}|N_d|LT)$$

Once created, the RREP is unicast to the next hop toward the originator of the RREQ, as indicated by the route table entry for that originator. As the RREP is forwarded towards the node which originated the RREQ message, the Hop Count field is incremented by one at each hop. Thus, when the RREP reaches the originator, the Hop Count represents the distance, in hops, of the destination from the originator.

5.4 TIER 1 SECURITY

The Tier 1 security is implemented at the route discovery process of TTSAODV. This tier is established, only when the RREP is from the intermediate node, that is, case A. At this level, the nodes before and after the intermediate node, this sends the RREP in the particular RREP, exchange verification messages, to check the authenticity of the route.

5.4.1 Sending Verification Message

During the Route reply process, upon receiving RREQ, if any intermediate has a fresh enough route to the particular destination, it sends the
RREP through the reverse path set by the RREQ. When the RREP reaches
one hop in the reverse path, that is, the previous node with IP address AD_P, it
sends a verification message to the next hop of the intermediate node AD_N
either through AD_I or through some other route according to the availability
of other route. The format of the verification message is given below:

\[
VM = AD_P | AD_N | AD_S | AD_D | Seq_{UD} | MAC(K_PN, AD_P | AD_N | AD_S | AD_D | Seq_{UD})
\]

where K_PN denotes the secret key shared by Previous node P and Next node N
of intermediate node. If the propagation of this verification message is
through an alternate path, then there is no possibility in identifying this
verification process by the AD_I. But, due to non-availability of the alternate
path, the previous node may send this verification message to the next hop
node through the AD_I. Then the intermediate can identify this verification
process. If AD_I is not a malicious node, it will co-operate with the verification
process by forwarding the verification message to the next hop node. But, if
the AD_I is a malicious node and if it tries to disturb the route discovery
process, it may either drop the route verification message or change in the
content of it by impersonating it as the next hop.

If the malicious node tries the first choice, that is, instead of
forwarding the verification message to the next hop, it simply discards it. But,
the previous node after sending the verification message will wait for the
verification reply only for certain duration. Within this duration, if the
verification reply is not received, then the previous node will send the
verification request message again. Even for the second verification message,
if the verification reply is not received, then AD_I is assumed as a malicious
node and it will be black listed.

The second choice of impersonating is not possible, because the
verification request and the verification reply are authenticated using MAC.
Only when the secret key shared between the previous node and the next node of AD is compromised by AD, this type of impersonation is possible. When a strong key management system, as per our assumption, is used, this problem can be avoided.

### 5.4.2 Sending Verification Reply

When the next hop of AD receives the verification request message for the previous node, it sends the verification result within a stipulated time to the previous node as follows:

\[
VR -> AD_P|AD_N|AD_D|Seq|UD|R_{\text{verify}}|MAC(K_{PN} | AD_P|AD_N|AD_S|AD_D|Seq|UD|R_{\text{verify}})
\]

where R\text{verify} is the result of verification. If the node N has the fresh enough route to the destination, then R\text{verify} is TRUE. Otherwise it is FALSE. If the verification result is TRUE, then the previous node sends the RREP to the source node. Otherwise, the RREP from the intermediate node is dropped and the intermediate node is listed in the black hole node, since it gives the false information regarding the fresh enough route.

### 5.5 TIER 2 SECURITY

According to the proposed protocol, all of the single black hole attacks are identified at the tier 1 itself. But, when the neighbours of the intermediate node that is, both the previous node and the next node of AD, from which RREP has been received are collaboratively acting with Black hole node, it is not detected in the tier 1. So, there is a need of second level of mitigation. This tier is started after establishing the route from the source node to the destination node through AD and after starting the data transfer.

In this tier, it is assumed that, the source node is sending \( R_m \) number of data packets per second to the destination node termed as message
rate. Along with the data packets, the source node also sends the control message to detect the black hole node at a rate of $R_c$. In this proposal, $R_c$ can be chosen randomly and it will be much smaller than $R_m$ in order to reduce message overhead. The control message asks the destination to send the acknowledgement and the size of the packet of control message is equal to that of the original message. So that, attacker cannot differentiate the original message and the control message.

The format of the control message sent by the source to the destination is as follows:

$$S \to AD_s|AD_d| N_s|MAC(K_{SD}, AD_s|AD_d| N_s)$$

Upon receiving and identifying the control message, the destination node sends the acknowledgement as follows:

$$D \to AD_d|AD_s| N_d|MAC(K_{SD}, AD_d|AD_s| N_d)$$

If the source node receives the acknowledgement within the threshold time, and it passes the verification through MAC, the route is decided to be secure against black hole attack. Only the destination node can create the correct MAC using $K_{SD}$, since only the source node and the destination node holds the secret key $K_{SD}$. If the acknowledgement is not received within the threshold time, the source node sends further control message more frequently at a message rate $R_c'$, where $R_c < R_c' < R_d$.

The control message could be lost either because of the black hole attack or because of the collision. So sender node will wait for the acknowledgement for three control messages. Even after sending three control messages, if the acknowledgement is not received, then the source node can be sure that the route is not secure against black hole attack. Thus the route
will be avoided for further data transfer. Figure 5.5 shows the flow of operation in tier 2 security.

![Flow Chart of Tier 2 Security](image)

**Figure 5.5 Flow Chart of Tier 2 Security**

### 5.6 COST ANALYSIS

Since the conventional AODV is enhanced with authentication algorithm and with the exchange of verification messages, it leads to additional cost both in computation and in communication. This section gives the cost analysis of the proposed protocol TTSAODV in terms of operations involved in the computations and communication for a single route discovery process.
5.6.1  Computational Cost

Computational cost is measured at every node in the network. Since every node in the mobile AdHoc network can be looked upon as both the sender and the receiver, the total computation cost incurred at each node is going to be the cost of this node being a sender plus the cost of the node being a receiver. Here ‘M’ denotes the Cost of computing a MAC.

The proposed scheme only involves the operation of MAC and with no signature at all. So, the additional cost consumed by the security addition is negligible. Table 5.1 shows the comparison of the computational cost at each node for a single route discovery process.

Table 5.1 Comparison of Computational Cost

<table>
<thead>
<tr>
<th>MAC Computational cost</th>
<th>RREP is from the destination</th>
<th>RREP is generated by any intermediate node</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TTSAODV</td>
<td>TTSAODV</td>
</tr>
<tr>
<td>At source node</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>At destination node</td>
<td>M</td>
<td>-</td>
</tr>
<tr>
<td>At the previous node</td>
<td>-</td>
<td>M</td>
</tr>
<tr>
<td>At the next node</td>
<td>-</td>
<td>M</td>
</tr>
<tr>
<td>Total Cost</td>
<td>2M</td>
<td>3M</td>
</tr>
</tbody>
</table>

Table 5.1 shows that, for a single route discovery, the algorithm TTSAODV consume a maximum of 3M computations additionally.

5.6.2  Communication Cost

Security never comes at free of cost. When more security features are introduced into the network, in parallel with the enhanced security strength, the computation, communication, and management overhead are
also increased (Hao Yang et al 2004). Communication cost involves the sending RREQ, RREP and verification messages. Table 5.2 shows the comparison of communication cost for a single route discovery process. Here, B denotes Communication cost of broadcasting and U denotes Communication cost of Unicasting by a mobile node.

**Table 5.2 Comparison of Communication Cost**

<table>
<thead>
<tr>
<th>Description</th>
<th>RREP is from the destination</th>
<th>RREP is generated by any intermediate node</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AODV</td>
<td>TTSAODV</td>
</tr>
<tr>
<td>Broadcasting RREQ from the source node</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Unicasting RREP from the destination node</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>Cost of broadcasting RREQ (at the worst case N-2 intermediate nodes)</td>
<td>BX (N-2)</td>
<td>BX (N-2)</td>
</tr>
<tr>
<td>Cost of broadcasting RREP (at the worst case N-2 intermediate nodes)</td>
<td>BX (N-2)</td>
<td>BX (N-2)</td>
</tr>
<tr>
<td>Unicasting Verification Request</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Unicasting Verification Reply</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td>BX (2N-1)+U</td>
<td>BX(2N-1)+U</td>
</tr>
</tbody>
</table>

From the table, it is seen that, the additional communication cost in the proposed protocol is only 2U+B when compared with the traditional AODV for a single route discovery process.
5.7 SUMMARY

Till date, all MANET security strategies need modifications on either network protocols or network topology, which may not be feasible for an operating commercial MANET. Even a current state of the art protocol or a successfully updated protocol may face DoS attacks armed with newer technologies in the future. Therefore, a new practical problem approach is demanded to defend MANETs against black hole attack. Thus, cryptographic authentication based enhancements on the conventional routing protocols AODV and AOMDV against black hole attack, TTSAODV and TTSAOMDV have been proposed. In order to reduce the control message overhead, a modified authentication algorithm is used. The cost increase in the proposed protocols is very less, which is acceptable by MANET. Since, two levels of security are provided in these protocols, the black hole attack is easily identified and rectified immediately. The proposed secure strategy runs on a MANET with AODV and AOMDV routing protocols. The experiment is implemented in the NS-2 network simulation environment because NS-2 simulator is widely applied and it is validated and verified.