The Secure Dynamic Source Routing Protocol in MANET using MD5 Hash Function

Radha S. Savankar
Email ID: radha_savankar@yahoo.co.in

Prof. S. V. Dhopte
Email Id: sanjaydhopte@gmail.com

Abstract - Dynamic Source Routing (DSR) is a routing protocol designed specifically for use in mobile ad hoc networks. The protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. When using source routing, each packet to be routed carries in its header the complete, ordered list of nodes through which the packet must pass. A key advantage of source routing is that intermediate hops do not need to maintain routing information in order to route the packets they receive, since the packets themselves already contain all of the necessary routing information. This, coupled with the dynamic, on-demand nature of Route Discovery, completely eliminates the need for periodic router advertisements and link status packets, reducing the overhead of DSR, especially during periods when the network topology is stable and these packets serve only as keep-alives.

Keywords - Dynamic Source Routing

I. INTRODUCTION

An adhoc network has a certain characteristic, which imposes new demands on the routing protocol. The most important characteristics are the dynamic topology, which is a consequence of node mobility. A mobile ad-hoc network (MANET) is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. The principle behind mobile adhoc networking is multi-hop relaying, which means messages sent by source to destination are forwarded by the other nodes if destination node is not directly reachable. In other words, an ad hoc node in MANET operates as not only end terminal but also as an intermediate router. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. Thus, multi-hop scenario occurs. In the absence of a security mechanism, it is easy for an attacker to insert, intercept or modify the messages. This means that unprotected MANETs are vulnerable to many attacks [8] such as wormhole attack [9], black hole attack [10] including node impersonation, message injection, loss of confidentiality etc.

Fig. 1.1 Structure of MANET

In ad hoc networks, the routing protocols are divided into three categories: Proactive, Reactive and Hybrid to avoid different attacks. Mobile ad hoc routing protocols can be classified in many ways depending upon their route construction and maintenance mechanisms, route selection strategy, topology formation, update mechanism, utilization of specific resources, type of cast, etc.

Fig. 1.2 Classification on Adhoc Routing Protocol

II. LITERATURE REVIEW & RELATED WORK

Many of the security solutions to secure the routing in MANETs have been proposed. Some research papers which focus on secure routing in mobile ad hoc networks are discussed below:

P. Papadimitratos and Z. Haas [3] proposed a secure routing protocol (SRP). SRP is based on a pre-share key between source and destination nodes. In SRP, a source node generates RREQ message and broadcasts it to its neighbors. When destination node receives RREQ message it verifies the source node and establish the route. Drawback of SRP is that it does not authenticate intermediate nodes. Author of [6] have shown the attack against the SRP protocol. In SRP...
protocol, an attacker can disrupts the normal functioning of this routing protocol in between source and destination nodes. Y.C. Hu, A. Perrig, and D. B. Johnson [4] proposed a secure routing protocol Ariadne. Ariadne protocol uses message authentication code (MAC) to maintain the message integrity and digital signature for authentication. In Ariadne protocol, the source node generates the route request (RREQ) message and append a hash value to RREQ message. Each intermediate node appends its identifier, digital signature and per hops value. When destination node receives RREQ packet it verifies source node and intermediate nodes, then sends back RREP message. Drawback of Ariadne is that it vulnerable to an active 1-1 attack [4], where an attacker could delete the node’s signature to forge a nonexistent route. L. Buttyan and I. Vajda [6] proposed a new protocol EndairA. They enhanced the security of Ariadne protocol proposed in [4] against active 1-1 attack [4] by providing security by appending the signature of source, destination and intermediate nodes. But EndairA protocol is vulnerable to active 0-1 attack [4] which is called Man in the Middle (MITM) attack. J. Liu, F. Fu, J. Xiao and Y. Lu [5] proposed EndairALoc protocol. The authors of [5] have shown that the EndairA [6] protocol is vulnerable to Man in the Middle (MITM) attack. EndairALoc protocol uses the pair wise pre-shared symmetric keys to construct the message authentication code (MAC) rather than public keys, randomly generated request identifier.

III. DYNAMIC SOURCE ROUTING

Unlike AODV and DYMO, DSR is a source routing protocol. This means that the source node adds the whole route up to the destination node to the packets header (Figure 3.1). As this is the case with most reactive ad hoc routing protocols, DSR is based on the two basic mechanisms namely route discovery and route maintenance. During the route discovery a route is set up on-demand. The route maintenance monitors an established connection during a communication between nodes [2]. DSR is able to operate on networks containing unidirectional links but it works optimal in a network with bidirectional links.

<table>
<thead>
<tr>
<th>Option Type</th>
<th>Option Data Length</th>
<th>Identifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address[1]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Address[2] | | *
| .................. | | |
| Address[n] | | |

Fig. 3.1: DSR data packet header format

A. DSR Basic Functions

If a source node originates a new data packet to some destination node, it adds the whole path “source route” in the packet header. The source node searches for a route to that destination in its own route cache table (Figure 3.2). If it does not find an entry, it initiates a route discovery process to dynamically find a route to the destination node. Route discovery is similar to that in AODV. However, there are some differences. First, the RREQ packet (Figure 3.3) broadcasted by a source nodes include a new field, the route record, which saves the nodes the RREQ packet traverses on it travels towards the destination node. Second, intermediate nodes receiving the RREQ check if their address is included in the route record. Third, if the RREQ packet arrives at the destination node, it checks its route cache for another route to the source node. If it finds one, the destination node generates a RREP packet (Figure 3.4), adds the route record (from RREQ packet) and sends the RREP back to the source node over its own route. Therefore DSR can work in a unidirectional link field where the revise route is not available and using other routes for replying to the RREPs. Otherwise, the destination node sends the RREP packet over the reverse route back to the source node. The route maintenance is processed as mentioned in AODV. If an intermediate node could not forward a data packet, it generates a RERR packet (Figure 3.5) and sends it back to the source node. Whenever a node receives a RERR message, it deletes all its routes containing the broken link.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Source Route Record</th>
<th>…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address (1)</td>
<td>Address (2)</td>
<td>… Address (i)</td>
</tr>
</tbody>
</table>

Fig. 3.2 DSR route cache table packet format

<table>
<thead>
<tr>
<th>Option Type</th>
<th>Option Data Length</th>
<th>Identifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address[1]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Address[2] | | *
| .................. | | |
| Address[n] | | |

Fig. 3.3 DSR RREQ packet format

<table>
<thead>
<tr>
<th>Option Type</th>
<th>Opt Data Length</th>
<th>L</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address[1]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Address[2] | | | *
| .................. | | | |
| Address[n] | | | |

Fig. 3.4 DSR RREP packet format


<table>
<thead>
<tr>
<th>Opt Type</th>
<th>Opt Data Length</th>
<th>Error Type</th>
<th>Rsvd</th>
<th>Slavage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3.5 DSR RERR Packet Format

**B. Additional Features**

In addition to the two basic mechanisms mentioned above, DSR protocol provides further features.

**B.1 Route Discovery Features**

- **Caching Overheard Routing Information**
  
  If a node is forwarding or overhearing any routing packet it updates its own route cache.

- **Replying to Route Requests Using Cached Routes**

  If an intermediate node receives a RREQ packet to other destination and has a valid route to the requested destination, the intermediate node unicasts a RREP packet back to the source node.

- **Route Request Hop Limits**

  Each RREQ packet contains a "hop limit" or time-to-live “TTL” field in its IP header. The TTL is used to limit the propagation of the RREQ packet with the aim to reduce the routing control packets overhead on the network.

**B.2 Route Maintenance Features**

- **Packet Salvaging**

  Packet salvaging occurs if an intermediate node forwarding a data packet detects that the link to the next node is broken and it has another valid route to the destination in its route cache. Otherwise, the node drops the data packet. In all cases, the node sends back a RERR packet toward the source node.

- **Automatic Route Shortening**

  If a node is able to overhear a packet carrying a source route, which will come to it later, the node should send back a RREP with the shorter path to the source node.

- **Increased Spreading of Route Error Messages**

  If a source node receives a RERR, it propagates this RERR to its neighbors by including it in its next RREQ. In this way, the source node does not respond with a new RREP contain the same invalid link.

**IV. MD5 HASH**

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

The MD5 hash also known as checksum for a file is a 128-bit value, something like a fingerprint of the file. There is a very small possibility of getting two identical hashes of two different files. This feature can be useful both for comparing the files and their integrity control.

**A. MD5 Hash Properties**

The MD5 hash consists of a small amount of binary data, typically no more than 128 bits. All hash values share the following properties:

- **Hash length**

  The length of the hash value is determined by the type of the used algorithm, and its length does not depend on the size of the file. The most common hash value lengths are either 128 or 160 bits.

- **Non-discoverability**

  Every pair of nonidentical files will translate into a completely different hash value, even if the two files differ only by a single bit. Using today's technology, it is not possible to discover a pair of files that translate to the same hash value.

- **Repeatability**

  Each time a particular file is hashed using the same algorithm, the exact same hash value will be produced.

- **Irreversibility**

  All hashing algorithms are one-way. Given a checksum value, it is infeasible to discover the password. In fact, none of the properties of the original message can be determined given the checksum value alone.

**V. PROPOSED SECURE ROUTING PROTOCOL**

In our protocol, when a node wants to communicates, it initiates route discovery process by generating a RREQ message. Source appends its digital signature (DS) to the message. Neighbors of source first verify the signature of source and make the decision accordingly. We added a one way hash function to the RREQ message to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route list of RREQ message can be detected. Destination sequence number [12] in the protocol is added to make the loop free routing and to check the freshness of route control packet. Assume that S is the source node trying to discover a route to destination D and route from S to D exist via intermediate node M and N.

**A. Assumptions are**

1) The nodes which are within range of each other are neighbors.
2) All the nodes in network have their own public and private key pair generated by any key management system for mobile ad hoc networks.
3) Public key of nodes are known to others nodes in network.

B. Notations are

1) LI Life time (maximum number of hop) of a packet ‘I’.
2) Seq Destination sequence number.
3) DSA Digital signature of node A.
4) hA Hash value appended by node A to the message.
5) A *, node A broadcast a message.
6) B, node A sends a message to node B.

C. Operation of proposed protocol and format of RREQ and RREP messages

1.) S-> * RREQ <Seq, S, D, LREQ, <>, DSs, hS>
2.) M-> * RREQ <Seq, S, D, LREQ-1, <M>, DSs, DSM, hM>
3.) N-> * RREQ <Seq, S, D, LREQ-2, <M, N>, DSs, DSM, DSN, hN>
4.) D-> N: RREP <Seq, S, D, <M, N>, DSs, DSM, DSN, DSD, hD>
5.) N-> M: RREP <Seq, S, D, <M, N>, DSs, DSM, DSN, DSD, hD>
6.) M-> S : RREP <Seq, S, D, <M,N>, DSs, DSM, DSN, DSD, hD>

D. Description

The operations of protocol are shown above. A source S initiates route discovery by generating route request (RREQ) message. RREQ contains the address of source and destination, Seq, LREQ, route list of intermediate node which makes the route from source to destination (initially empty), digital signature of source DSS, and a hash value hS. Life time of a packet refers to maximum number of hop which a packet can travel. On each broadcast, life time would be reduced by one automatically. If life time is reached to zero, packet would be discarded. Source produced the hS using one way hash function.

hS = H(S, D, Seq, LREQ) ..........................(1)

When a neighbor of S, M receives the RREQ message, it verifies the signature of source node. If source node is genuine node, M checks Seq and compare with Seq stored in its cache. If Seq is less M discards the packet. Otherwise, it appends its identifier to route list and digital signature DSM to the message and replaces the hS by hM and then rebroadcasts

hM = H(hS, M, LREQ-1)............................(2)

Similarly, node N verifies signature of source and node M and checks Seq, and then appends its identifier to route list and digital signature DSM to the message, replaces the hM by hN and finally rebroadcasts.

\[ hN = H(hM, N, LREQ-2) \] ..........................(3)

Finally, when destination node D receives the RREQ message, it verifies all the signatures contained in RREQ packet, compares Seq with previously stored Seq in its cache. If source and all the nodes in route list are genuine and packet is not outdated, the destination node, it computes:

\[ hD = H(N, LREQ-2, H(M, LREQ-1, H(S, D, Seq, LREQ))) \] ..........................(4)

and compares the value of hD with hN. If both values are same, the message integrity is verified. Otherwise message is discarded. If all the verifications are successful, the destination D creates a route reply (RREP) message and sends back to the source S via the path obtained by reversing the route list in RREQ packet. Route Reply (RREP) message contains Seq, addresses of source and destination, route list, hD, and signature of all the nodes from source to destination. Each intermediate node verifies the signature of destination D and Seq to check the freshness of message. On receiving RREP message at source, S verifies signature of all the nodes in route list and Seq. Source S computes:

\[ h = H(N, LREQ-2, H(M, LREQ-1, H(S, D, Seq, LREQ))) \] ..........................(5)

and compares with hD to check the integrity of route list. If both values are same, S accepts RREP. Otherwise discards. S calculates the values of LREQ-1 and LREQ-2 on the basis of route list. After successful completion of all verifications, a route from S to D is established.

IV. CONCLUSION

The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. In this paper, I have proposed a protocol to secure on demand source routing in MANETs that fulfills the security requirements. Our protocol uses one way hash function to maintain the integrity of message. Therefore, deletion of a node from or any kind of modification in route control packet can be detected. Using Public Key Cryptography (PKC), nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Source, destination and intermediate nodes in route list authenticate others nodes by verifying signature. Our protocol is based on Public Key Cryptography. Therefore, it consumes much battery power than protocols based on symmetric algorithms.

DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even
with continuous, rapid motion of all nodes in the network. DSR operates entirely on demand [12], with no periodic activity of any kind required at any level within the network. This entirely on-demand behavior and lack of periodic activity allows the number of routing overhead packets caused by DSR to scale all the way down to zero. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use.

REFERENCES


AUTHOR’S PROFILE

Radha S. Savankar
Department of Information and Technology
ME (IT) 1st year
Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati
Email ID: radha_savankar@yahoo.co.in

Prof. S. V. Dhopre
Assistant Professor
Department of Information Technology
Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati
Email ID: sanjaydhopre@gmail.com