A STUDY ON SECURITY LEVEL OF AD HOC ROUTING PROTOCOL TO FIND OTHER APPROACH WITH DSDV

Prof. Vikram M. Agrawal¹, Prof. Samip A. Patel²
IT Department, BVM Engineering College

ABSTRACT

Mobile ad hoc networks have a collection of large number of mobile nodes that form temporary network without aid of any existing network like physical infrastructure or central access point. So it means in MANET it can not be identified the particular topology for particular time. The main characteristics of MANETs are dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability. These all properties make it completely different from other network. Due to such properties of MANETs, to design and development of secure routing is challenging task in open and distributed communication environments with protocols. There is option of cryptography to give advance security to already present protocols. It may be best option of DSDV for key management and message sending.

Keywords: MANETs, Security, Cryptography, DSDV, AODV.

1. INTRODUCTION

WIRELESS cellular system has been in use since 1980s. At the starting of the development of wireless system, it operates with the help of a centralized supporting structure it means there is one server or main point which manage the all the network. This is also known as an access point. Recent advancement of wireless technologies like Bluetooth [3], IEEE 802.11 [4] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1, 2, 5, 6], which operate in the absence of central access point or server. It provides high mobility and device portability that enable to nodes connect network and communicate to each other anytime and anywhere. It allows the devices to maintain connections to the network as well as easily adding and removing from the network. User has great flexibility to design such a network which is available at cheapest cost and minimum time. DSDV is the only proactive protocol taken for comparison with other secure protocols. It has most common features with the traditional routing protocols in wired networks. The sequence numbers are added to ensure loop-free routes.
2. FEATURES OF MANETs (Different type of connection)

A mobile ad hoc network has following features [7]:
- Autonomous Terminal: It means each node may function as both a host and a router. So each node can send and receive packet as well work as mediator.
- Distributed Operation: The nodes act as a relay to implement functions. So packets are sent in form of relay one will send packet to second and second will send to third and so on.
- Multi-hop Routing: When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate node [8]

![FIG 1: Multi Hop Routing](image)

- Dynamic Network Topology: The mobile nodes in the network dynamically establish routing among themselves. When they finish the work then loose the network and move out
- Light-weight Terminal: In this network is established for some particular purpose. In these MANET nodes with less CPU processing capability, small memory size, and low power storage are exist.

3. WEAKNESSES OF MANETs

Since nodes in mobile network can move dynamically, the network tends to change its topology very frequently just because of joining and leaving network is not managed by any central entity. This mobile nature of the nodes may create many security and other issues in MANETs [7]:

- Lack of Centralized Management: It is impossible to detect attacks.
- Infrastructure less: Detecting faults in network is not easy. There is dynamic and free feature for each node in ad hoc network so fault is not detected.
- Dynamic Topology: Results in weaker relationship among nodes. Not easily find out about how many nodes in network at present.
- Packet Loss: Mobility of nodes, bit rate error and interference causes packet loss.
- Mobile Nodes: It is easy for malicious nodes to enter any network and hinder communication.
- Security: Mobile nodes itself perform the major networking tasks, so it is easy for any attacker to acquire data or pretending to be authorised node.
- Resource Availability: Providing security in mobile network requires various resources and architectures.
4. ROUTING IN MANETS

The choice of the route being selected is done by the routing algorithm [11]. As in Fig 2 it is clearly shows the classification of the routing protocols.

**FIG 2: DIFFERENT ROUTING PROTOCOLS IN Manets**

4.1 Reactive protocol

Reactive protocols are also called on-demand protocols because they maintain or discover route only on demand or required [11]. A control message is flooded to the routes to discover the appropriate route. It only establishes the route when any node in the network wants to send a message or a packet to another node in the network. The advantage of these protocols are that it reduces the routing table overflow and its major disadvantage is that due to its on demand nature while route discovery a longer delay is been found. The example of this type of protocol are DSR (dynamic source routing), AODV (ad hoc on demand distance vector routing), LAR (location aided routing), TORA (temporally ordered routing algorithm). These types of protocol maintain the details when it is required to send packets. So this is good when there are many dynamic nodes are available in one ad hoc network.

4.2 Proactive protocol

Proactive protocols are also named as table driven routing protocol. They maintain the routing table of the entire network constantly like where the packets are sent, how they sent and which route are used to send packets. Each node has to maintain one or more tables to store routing information and also response to changes in network topology by broadcasting acknowledgement and propagating [12]. The routing tables are constantly updated whenever the network topology changes. Each node in the network sends a broadcast message to the entire network if there is any change in the network topology. This feature of maintaining routing entries of the entire network may affect the routing table but it provides the actual information of the entire network. For very large network the proactive routing protocols may not be recommended because they maintain...
entries of each node in the network which causes more bandwidth consumption and overload to routing table. The examples of proactive routing protocol are DV (distance vector), DSDV (destination sequence distance vector), OLSR (optimised link state routing), and WRP (wireless routing protocol) which is an enhanced version of DSDV.

4.3 Hybrid protocols
As according to the name hybrid routing protocols are a combination of both reactive and proactive routing protocols. Basically to overcome the shortcomings of reactive and proactive routing protocol the hybrid is used. It uses the route discovery and on demand mechanism of reactive routing protocol and the routing table management mechanism of proactive routing protocol. In hybrid routing protocol a large network is divided into zones. The routing inside the zones is done by using reactive approach and the routing outside the zone is done using reactive approach. [13] It is the most effective and appropriate routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state).

<table>
<thead>
<tr>
<th>TABLE 1: Comparison of Proactive, Reactive and Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages</td>
</tr>
<tr>
<td>Proactive</td>
</tr>
<tr>
<td>• Up-to-date routing information</td>
</tr>
<tr>
<td>• Quick establishment of routes</td>
</tr>
<tr>
<td>• Less delay</td>
</tr>
<tr>
<td>• Routing information not fully used</td>
</tr>
<tr>
<td>Reactive</td>
</tr>
<tr>
<td>• Saving resources</td>
</tr>
<tr>
<td>• Reduces routing load</td>
</tr>
<tr>
<td>• Loop free</td>
</tr>
<tr>
<td>Hybrid</td>
</tr>
<tr>
<td>• Scalability</td>
</tr>
<tr>
<td>• Limited search cost</td>
</tr>
<tr>
<td>• Up-to-date routing information within zones</td>
</tr>
</tbody>
</table>

5. METHODS TO SECURE ROUTING PROTOCOLS

AODV does not take security into account. AODV messages are neither encrypted nor authenticated nor integrity protected. So it is basically always assumed as trusted. Based on the possibility to forge packets and on the distributed and uncontrolled nature of the network many attacks are possible. Because of forge packets, destination can not identify the integrity of the message or packets. Due to these reasons many security techniques should be implemented on AODV. There are some following techniques provide security to ad hoc routing protocols.
SAODV: - Secure AODV is an extension to AODV routing protocol. It is proposed by M. Zapata and N. Asokan. It is based on public key cryptography and hash algorithm. SAODV routing messages (RREQs, RREP, and RERRs) are digitally signed, in order to guarantee their integrity and authenticity [14]. So we can easily identify that is there any unauthorised activity is placed or not. There is a key management system which makes it possible for each node to obtain public keys from the other nodes of the network. How this is achieved depends on the key management scheme. There are different approaches for key management. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate, and hash chains to secure the hop count information (the only mutable information in the messages). For the non-changeable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the changeable information. To preserve the collaboration mechanism of AODV, SAODV that allows intermediate nodes to reply to RREQ messages, when any node want to send message. This is called the double signature to get idea of authenticated source when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a pretended RREP message towards intermediate node itself.

A-SAODV – Adaptive secure AODV is another approach to secure AODV routing protocol from attacks and from malicious users. It is based on the AODV-UU implementation by Uppsala University. Unlike AODV-UU, A-SAODV is a multithreaded application [15]. In A-SAODV, there are two execution threads: one carries the cryptographic operations and the other to all other functions (routing message processing, SAODV routing table management, timeout management, SAODV message generation, and data packet forwarding). The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. [15]

SEAD – Secure efficient Ad hoc distance vector is a proactive routing protocol. It is another routing protocol which is secure as it is based on one way hash functions to provide authentication. Each node contains its individual hash chains which are separated into segments to prevent an attacker to forge sequence numbers [16]. So with this sequence number we can identify that there is some unauthorised message in between in actual packets.

ARIADNE - It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig based on DSR. It is a secure on-demand routing protocol that can authenticate messages using one of the three ways: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signature[16]. In shared secrets key two nodes (source and destination) mutually and securely share the key so no one can open the key. In second method there is disadvantage of broadcasting of secret key because if any unauthorised nodes to pretend real actor then he can also get broadcasted secret key. The third method provides more security then other two methods because by digital signature, we can easily identify the person is authorised actor or not.

ARAN - It is proposed by Dahill. Authenticated Routing for ad hoc networks detects the attacks from malicious nodes and also protects the network from forged actions. It uses cryptographic certificates for authentication purpose. The certificate includes the IP of the node, the public key of the source node, a timestamp of the time at which the certificate was created and another timestamp of the time at which the certificate expires. So by using the timestamp user or node can use particular certificate for particular time. The disadvantage of timestamp is that suppose some packet takes less time as per valid time certificate then an intruder can use certificate to send the forge packets. This is the first step which is covered. After the successful completion of the first step second step is preceded. It discovers the shortest path to the destination. It is an on-demand routing protocol. It is successful in protecting the network against impersonation attack but is vulnerable to wormhole attack. [16]
6. RELATION BETWEEN ATTACKS AND PROTOCOLS

Relation between attacks and different security protocols is shown in table 2.

**TABLE 2: Relation between Attacks and Protocols**

<table>
<thead>
<tr>
<th>PROTOCOLS</th>
<th>ATTACKS</th>
<th>SAODV</th>
<th>SEAD</th>
<th>ARIADE</th>
<th>ARAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLACK HOLE</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>SPOOFING</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>WORMHOLE</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

7. CONCLUSION

In conclusion we can say that there is some ambiguity to provide security in reactive protocol AODV and proactive protocol SEAD. If we provide some functionality to DSDV then we can best option for key management and sending packets. The table in section 6 indicate that there is possiblility of attack in SAODV, SEAD, Ariadne, and ARAN. There is another approach to provide security with DSDV. DSDV is the only proactive protocol taken for comparison. It has most common features with the traditional routing protocols in wired networks. The sequence numbers are added to ensure loop-free routes. If we short out the problem of mobility and join the protocol in long time then DSDV can be best approach for key management and sending packet then other protocols.

8. REFERENCES


