SRAAA : A SECURE ON-DEMAND ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

Capt. Dr. S. Santhosh Baboo¹, V J Chakravarthy²

¹Associate Professor, ²Research Scholar, Dept. of Computer Science, D.G Vaishav College, Arumbakkam, Chennai-106 (India)

ABSTRACT
As we already know, the nodes in mobile ad hoc networks act both as regular terminals (source or destination) and as routers for other nodes in the network, unlike fixed wired networks, such as the Internet, where dedicated routers are controlled by a service provider. In mobile ad hoc networks, provision of security becomes a challenging task in these networks, because of the absence of dedicated routers. The task of ensuring secure communication in the mobile ad hoc networks is difficult for reasons including the mobility of nodes, limited processing power and limited availability of resources, such as battery power and bandwidth. Mobile ad hoc networks rely on the collaboration of the nodes involved for the network to create itself and operate efficiently. While maintaining suitable routing information in a distributed way is a challenging issue in such networks, it is even more challenging to secure the protocols used for routing. At the network level, the mobile ad hoc network fundamentally requires secure routing protocols, as these enable a communication path to be established. On the other hand, most of the routing protocols designed for these networks give no consideration to security, operating with an implicit assumption of trust among the nodes. This provides opportunities for malicious attacker’s intent on bringing down the network. Many types of routing protocol exist and have been extensively researched, with a view of finding solution to security vulnerabilities. Our contribution presented in this paper is to design a secured Right angled and Ant search routing Protocol (SRAAA) for mobile ad hoc networks based on the integration of security mechanisms that could be applied to RAAA routing protocol. It proposes a novel secure routing protocol to improve the security level in mobile ad hoc networks, based on key management (RSA), Hash function and MD5 (digest algorithm), which protects data to satisfy our security requirements.

Keyword: MANET, Ant Search Method, Biased Geographical Routing, RSA, MD5.

I INTRODUCTION
Our contribution presented in the paper is to design a secured protocol named “Secured Right Angled And Ant search routing Protocol (SRAAA)” for mobile ad hoc networks which is based on the integration of security mechanism. This integration security mechanism is applicable for SRAAA routing protocol which proposes a secure routing protocol and also improves the security level in mobile ad hoc networks which is based on key management (RSA), Hash function and MD5. This key management, Hash function and MD5 protects data to satisfy our security requirements.
II RIGHT ANGLED BIASED GEOGRAPHICAL ROUTING AND ANT SEARCH PROTOCOL

RAAAA protocol is a multipath routing protocol that works on on-demand routing scheme. Some important features are added to the RAAA protocol to overcome the disadvantages of multipath protocols. These features improves the performances providing stability and availability required to guarantee the selection of the best path and also to reduces the congestion effects, the occurrence of broken links and dropped packets. The congestion control mechanisms BPNS and NNPS are used to reduce the congestion during transmission of packets that highly enhances the RAAA protocol.

III SRAAA PROTOCOL

SRAAA is a secured protocol that to protect data transmission and to construct a secure routing which is introduced to the RAA protocol. This SRAAA protocol mainly works on a group of mutually trusting nodes. Mutually trusting nodes are classified into two types namely Normal nodes and Special Nodes. Normal nodes are those nodes which are not involved in the packet transmission and the special nodes are those which are actively involved in packet transmission. This special nodes includes Source node, Intermediate node and the Destination node. At the time of transmission SRAAA functions into three stages namely Data Encryption stage, Secure routing protocol stage and Data Decryption stage. In Data Encryption stage and Data Decryption stage works only on key management and in case of secure routing protocol stage works only on Hash function and MD5 (digest algorithm). This three stages were explained below.

3.1 Data Encryption With Keys

In RSA algorithm Data Encryption occurs and keys are produced. The RSA algorithm approaches were made use in SRAAA protocol because of its superiority is distributing keys, achieving integrity and non-repudiation of data. The RSA algorithm produces two different keys namely public and private keys. Public keys are generated and distributed within nodes which are available in the network. The private keys are those keys which will be generated within the each node and will not be generated to the other nodes in the network. After encryption RAAA protocol produces two types of variables namely static and dynamic variables. After the production of two variables RAAA protocol works in three phases namely routing table, sequence table and effective routing path. These three phases are explained below:

3.1.1 Routing Table: When RAAA starts running, initially, the routing table will be created with the distance and angle for all the nodes with the public key which is participating in the network. It will check for the nodes which are in 90° degree from the source to destination through the intermediate node. This routing table is not a stable. it will dynamically change according to the network.

3.1.2 Sequence Table: It is used to find the possibilities of the route from the source node to destination node. i.e., the sequence table will have the multiple paths from source node to reach the destination node. This table will use to select the alternative path one the link has been failed or some malicious node will be there in the network. This sequence table is not a stable. It will dynamically change according to the network due to the mobility of nodes in the network.
3.1.3 **Effective Routing Path**: It will select the effective path from the sequence table from the source to destination node. This is the path the packets planning to go. This path is not a stable. It will dynamically change according to the network. This table contains the current path which is allowing the packets transmission from the source node to destination node.

After the routing table is created, sequence table will also be created from the routing table. Let us consider for the following figures 1.1(a), 1.1(d), 1.1(c), 1.1(d), indicating the possibilities for transmitting the packets from source node to destination node which have been in sequence table.

**1.1 (a) Routing Path involving four intermediate nodes from source node to destination node**

The figure 1.1(a) shows the packets where transmitted to the destination node from source node with four hop count, that to it takes only 90°, which is basic idea.

**1.1(b) Routing Path involving five intermediate nodes from source node to destination node**

The figure 1.1(b) shows the packets where transmitted to the destination node from source node with five hop count, from the figure we can understand that it takes more energy to transmit the packets. According to our problem, it is not the best effective routing path.
1.1(c) Routing Path involving four intermediate nodes from source node to destination node

The figure 1.1(c) shows the packets where transmitted to the destination node from source node with four hop count, from the figure we can understand that it takes four hop and also utilizes less amount energy to transmit the packets. According to our problem, it is one of the best effective routing path.

1.1(d) Routing Path involving five intermediate nodes from source node to destination node

The figure 1.1(d) shows the packets where transmitted to the destination node from source node with five hop count, from the figure we can understand it takes more hops and also it takes more energy to transmit the packets. According to our problem, it is not the best effective routing path.

From the above figure 1.1(a), 1.1(d), 1.1(c), 1.1(d), the figure 1.1(a) and 1.1(c) indicates the best path for transmission. But out of two, figure 5.1(a) has an effective routing path, since it utilizes less hop count and less energy.

3.2 MD5 – Digest Algorithm

It will create an ID, IP and MAC address for every node It will also create a private certificate for each and every node which is having the Node ID, IP, MAC, Encrypted message, private and public key.

The information in the each certificate

<table>
<thead>
<tr>
<th>Node ID</th>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash function</td>
<td>******</td>
<td>******</td>
</tr>
</tbody>
</table>
Example of certificate generated through MD5 algorithm to provide secured routing:

```
Node (13)
192.26.2.1
01bcbb824aa1d6fd6b9bf6ca4306b6ec
00:31:19:19:B1:EM
7
7
```

The above format will give the uniqueness. The malicious node can change the node ID, IP address, but cannot change the MAC address.

The above format will give the uniqueness, such that if any malicious node gets into the network environment while transmission of data. Any types the malicious node can change the node ID, IP address, but cannot change the MAC address since the malicious node getting the packets transmits to the another malicious node or transmits the packets to another node which are not participates in the transmission or simply drops the packets.

### 3.3 Hash Function

The Hash function is used to encrypt and update the data necessary for the routing process in order to secure the data. The hash function, using Node ID, IP Address and MAC address it will encrypt the message which is already encrypted by RSA by checking the certificate.

Now the data will be more secured, that is the MD5 itself will not know the data encrypted by RSA algorithm.

Now the data will contains the private key of the node and public key and also contains the encrypted message which is done by hash function.

\[
\text{(Data + Private Key) Public Key + Hash Function}
\]

#### 3.3.1 Secure Routing Protocol Stage – Link Level Security

In this stage of the protocol, after completing the above cycle in the source node, The RAAA will go the next effective route path for finding the next hop to transmit the data. During transmission, there may be possibilities of changing node information in the sequence table (Dynamic Variable i.e., the variable that can change be changed while transmission of data) and effective route path dynamically, since the entire nodes are mobile.

Based on the current effective route path table, it will select the next hop node to transmit the data.

Before transmitting the data, the MD5 will check the certificate of the next hop node. If the certificate is there in the node, the flag is set to one, it will give link to the next hop, then using TCP and UDP packets will be transmitted to the particular node. If the certificate is not there, the MD5 will check is that node is really in the network or network with the use of public key. If the public key is there for that node, the certificate will be generated by the MD5, and then transmission will be takes place. If the public key is not there, it will identify it as a malicious node and flag set as zero. If it is zero it will not give the link. Thus, the link level security will be created, before sending the data from one node to another node.

The above cycle will be continued till the data reaches the destination node, in the destination node.
3.3.2 Decryption Stage

Once the data / message reaches the destination node, the data / message contains all the private key, public key, hash function encrypt key. Using the RSA algorithm all the above key will decrypt using decryption process. Thus the original data will reach the destination node with more secured manner using the SRAAA protocol.

IV SIMULATION RESULTS
V CONCLUSION

The preliminary study has explained about secured routing protocol which is based on the key management, a secure path and protecting data to satisfy our security requirements. After understanding the security requirements and the types of attacks in mobile ad hoc network (MANET), the highly secured multipath routing protocol named SRAAA protocol were proposed which is based on the RSA cryptography, Hash Function, MD5 (Digest Algorithm) and time synchronization. All the mechanisms that are applied to the SRAAA protocol is to prevent external attacks including black holes and routing holes, additionally provides the viability, authentication and also saves energy at the time of effective work.

REFERENCES


