Self-Reconfigurable Secure Routing Method with AOMDV Protocol

T.Parameswaran¹, C. Palanisamy², P.Sathiya Devi³

¹Assistant Professor, Dept. of CSE, Anna University Regional Centre, Coimbatore.
²H.O.D, Dept of IT, Bannari Amman Institute of technology, Sathyamangalam.
³PG Scholar, Dept. of CSE, Anna University Regional Centre, Coimbatore.

Abstract: Secret communications are important for many applications in mobile ad hoc networks. AASR (Authenticated Anonymous Secure Routing) protocol is mainly used to defend the attacks in Mobile ad hoc network. In our studies, the route request packets are authenticated by using Onion routing and group signature. Onion routing with the route secret key authentication message is also used which defends the possible active attack without the introduction of node identities. Group signature can be used to legitimate the route request packets. In this paper, the existing protocols are too difficult to discover the link failure or node failure in the secure communication network. We proposed the novel secure routing protocol AOMDV (Ad hoc on demand multipath Distance vector routing) can be used to prevent the link failure for secure communication in MANETs. The ASR (Autonomous Network Reconfiguration system) algorithm can be used in the AOMDV protocol that enables a multi-radio wireless mesh network to recover the link failure to preserve the network. Simulation results have demonstrated the effectiveness of the proposed AOMDV protocol with improved performance as compared to the existing protocol.

Keywords: AASR, AOMDV , Group signature, MANET, Onion Routing


1 Introduction

Mobile ad hoc networks (MANETs) the nodes inside the network cannot be trusted at all times, since a valid node can be taken by the attacker and becomes malicious. The number mobile device can be used to form a network it does not need any other kind of fixed station or any existing infrastructure. MANET can be defined as an [1] autonomous system of nodes or mobile stations connected by wireless links, it forms a communication network model in the form of an unpredictable communication graph. In a MANET, no infrastructure exists and the network topology may change dynamically in a random manner since nodes are move and each node has limited transmitting power, restricting access to the node only in the neighbor range. MANETs are basically peer to peer, the information packets transmitted in a store and forward manner in multihop wireless networks from a source to an unpredictable destination, through intermediate nodes.

Two types of MANETs exist: open and closed [2]. Closed MANETs don’t have collaboration problems, since all nodes work towards a common goal and can easily be controlled. The nodes share the resources to ensure the connectivity in open MANET and to ensure global connectivity, but they may have different goals. The nodes in open multiple users operate the MANETs and they need not be forced to cooperate. However, the traditional fixed network routing protocols does not solve the major problems in mobile ad hoc network. The network topology can be frequently changed and to support the lack of fixed infrastructure. Such features pretense serious privacy issues for user and security threats for the information in an unfavorable environment. The user can communicate with each other, MANET routing protocols [2], [3] provide a route to the each user in the network. The MANET routing protocols are categorized by the following two types: reactive and proactive. Most of these routing protocols rely on collaboration between nodes because of the lack of a centralized administration and it also assumes that all nodes are authentic and reliable. These features of MANET provide an opportunity for a malicious user to introduce different kinds of attacks at the network layer with revere to routing. A malicious node may falsely advertise good paths to destination node[4] during the route discovery process it drops some selective packets and it reveal secret information to unauthorized nodes in the network, the network may consume away resources of other nodes and may interrupt the routing operation of the network. The protocols routing performance is degraded by malicious features. Anonymous routing protocols are important in MANETs that provide secure communications by hiding node identities and it will use for outside observers to preventing traffic analysis attacks from. MANETs includes identity and location anonymity of data sources and destinations as well as route anonymity. The requirements
of Anonymous communication in MANET can be described as a combination of unlinkability and unidentifiability. Unlinkability means the two nodes cannot be linked or the route between the source and destination cannot be recognized. Unidentifiability [5] the source and destination node identities are not revealed to the other node. The anonymous secure communication can be established by the route between the source, destination, and every intermediate node along the path. Many anonymous routing protocols proposed in the adversarial environment. Compare to the previews on demand protocols(ex. ANODR, SDAR, MASK) does not fully satisfy the unlinkability and unidentifiability problem in MANET. An Authenticated Anonymous, secure Routing protocol can be used to overcome the unlinkability and unidentifiability problem. Onion routing and group signature can be used in these secure communication networks. Onion routing can be used for route discovery and encrypt the route request –route reply verification message. The route request packets are authenticated by group signature, to prevent intermediate notes from modifying route packets. AASR routing protocol can be used for increasing the throughput and to experience more cryptographic operation delay. In this method we find malicious nodes of inside attack and outside attack, then provide secure routing but if in this secure routing has face any link failure occurred mean we face the data loss. To detect and avoid the link failure in a adversarial environment a possible trust based routing protocol can be combine with the existing protocol (e.g., AASR). The trust based routing can be more active to detecting the link failure problem in the communication network.

2. Related Work

In this section, we describe some anonymous secure routing mechanism and provide basic concept of existing system. The anonymous routing mechanism involve in the route discovery phase. In route discovery, the source node send the route request (RREQ) to the destination in the anonymous route request phase, and in the anonymous route reply phase the destination send the route reply (RREP) message to the source in the reverse path. 2.1 Anonymous Route Request

The source node S discovers the routing path to the destination D via the intermediate nodes. During the communication between the source and destination the intermediate node discover the identities of source and destination. The source node S broadcast the route request (RREQ) to the every node in the network.

\[
S \rightarrow * : \{RREQ, N_{seq}, V_{D}, V_{SD}, Onion(S)\}G_{S^{-}} \tag{1}
\]

Where RREQ is the packet type identifier; \(N_{seq}\) is a sequence number randomly generated by S for this route request; \(V_{D}\) is an encrypted message for the request validation at the destination node; \(V_{SD}\) is an encrypted message for the route validation at the intermediate nodes; Onion(S) is a key encrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key \(G_{S^{-}}\). The combination of \(V_{D}\) and \(V_{SD}\) works similarly to the global trapdoor used in ANODR. Introduce \(V_{SD}\):

\[
V_{SD} = (N_{i})K_{s} \tag{2}
\]

Where \(N_{i}\) and \(K_{s}\) are two parameters created by S and sent to D for future route verification; \(N_{i}\) is a onetime nonce for the route discovery; \(K_{s}\) is a symmetric key. The secret message \(V_{D}\) is defined as:

\[
V_{D} = (N_{v}, K_{v}, \text{dest})K_{SD}, \{K_{SD}\}K_{D}^{-} \tag{3}
\]

If S and D have already established \(K_{SD}\) in a previous communication, the costly public encryption in the second part of \(V_{D}\) can be eliminated, and then \(V_{D}\) is defined as:

\[
V_{D} = (N_{v}, K_{v}, \text{dest})K_{SD}, \text{pad} \tag{4}
\]

where Pad is a pre-defined bit-string that pads the message to a constant length. The encrypted onion Onion(S). S creates the onion core as follow:

\[
\text{Onion}(S) = O K_{s}(N_{seq}) \tag{5}
\]

Where \(N_{seq}\) is generated at a time the source S used to indicate itself. The core is encrypted with the symmetric key \(K_{s}\), and can be decrypted by destination D using \(K_{s}\).

<table>
<thead>
<tr>
<th>Req.Nym</th>
<th>Dest.Nym</th>
<th>Ver.Msg</th>
<th>Next_hop</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>(N_{seq})</td>
<td>(N_{D})</td>
<td>(V_{SD})</td>
<td>N/A</td>
<td>Pending</td>
</tr>
</tbody>
</table>

2.2 Anonymous Route Request

The Source forwarded route request packets are until it reaches the destination D in the network. The destination D receives route requests via the intermediate node J. Destination assembles the route reply packet and send back to the source node

\[
D \rightarrow *: \{RREP, N_{id}, (K_{v}, \text{Onion(J)})K_{JD}\} \tag{6}
\]

Where RREP is the packet type identifier; \(N_{id}\) is the route pseudonym generated by D; \(K_{v}\) and Onion(J) are obtained from the original RREQ and encrypted by the shared key \(K_{JD}\). The intended receiver of the RREP is J.

<table>
<thead>
<tr>
<th>Req.Nym</th>
<th>Dest.Nym</th>
<th>Ver.Msg</th>
<th>Next_hop</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>(N_{seq})</td>
<td>N/A</td>
<td>(V_{SD})</td>
<td>(N_{D})</td>
<td>Active</td>
</tr>
</tbody>
</table>

2.3 Onion Routing

It is an infrastructure for providing the private communication over a public network and is a bidirectional link. Permanent socket connections are established in the onion router in the network. The specific route message
with the core of an onion can be set up by the source node and a source node encrypts the route request message and sends to the destination through the intermediate nodes. The source and destination do not know the intermediate nodes ID’S. The destination node receives the onion and send back to the sources along the same path. The intermediate node can decrypt the route reply message and delete the onion outer layer. The destination address of onion routers treated as an anonymous data structure; thus, it is used to establish an anonymous connection.

### 2.4 Group Signature

In group signature each group member can sign the document behalf of the whole group and it provides the authentication without disturbing the anonymity. The group managers issue a pair of public and private keys to the every member in a group. Each member of a group can generate the own signature with its own private key, such signature can be verified by the other members in a group without revealing the signer’s identity. The signer’s identity can be traced by the group manager and to revoke the group keys.

### 2.5 AODV

Ad hoc on demand distance vector routing is a reactive protocol, it uses the control message to find the route from the source to destination, it begins a route discovery process to broadcast the route request packets. The AODV can also be used for e-broad cost a route request, it setup a reverse path routing towards the source. It is a bi-directional routing protocol. The destination receives a Route Request and, it sends the route reply along the reverse path setup when Route request is forwarded.

### 2.6 Anonymous On-demand Routing Protocol

ANODR is based on broadcasting with trapdoor information which includes many security mechanisms. ANODR is a topology based routing and broadcasting the information using public key. Anonymous route discovery and anonymous route maintenance are the two parts of the routing process in ANODR. It allows nodes to transmit packet to the source and destination without identity and it’s hard to discover the local transmitter.

### 3. Proposed Work

In the proposed system for recovering link failure or node failure in secure routing by using ARS algorithm. To form the Clusters first in this network and An Autonomous network Reconfiguration System (ARS) that allows node to autonomously reconfigure its local network settings-channel, radio, and route assignment for real-time recovery from link failures and then to reduce the data loss by using AOMDV protocol. AOMDV is the enhanced version of AODV protocol and it can be improved to compute the route cutoff problem in an effective manner, and compute more disjoint paths when source and destination pairs are distant separated. In this novel secure on demand protocol used to reduce the packet loss to increase the packet delivery ratio and also used to reduce the end-to-end delay in the communication network. It discovers the multiple paths between the source and destination, it does not have high inter-nodal coordination overhead, and it does not use the source routing to ensure the disjointness of alternate routes. It computes alternate paths with minimal additional overhead over AODV; it does this by exploit previously available alternate path routing information as much as possible. AOMDV based on hop-by-hop routing approach and it is based on the distance vector routing. AOMDV can be effectively managed the mobility induced route failure and it can use the route discovery procedure to find the on demand routes. The number of routes can be finding in the each route discovery in AOMDV. The Source forward the route request(RREQ) to the destination, it establishes the multiple reverse path at both the intermediate nodes as well as the destination, when using the AOMDV protocol. The destination receives the route request (RREQ) through the intermediate node and source using the same multiple reverse path. To reduce the occurrence of route discovery AOMDV provide the alternate paths to the intermediate nodes. In AOMDV, the route update can be used to maintain the loop-freedom and disjointness property.

### 3.1 System Architecture

The basic system architecture diagram shown in the figure(1). The system architecture shows how data is transferred from source to destination using AASR protocol in Mobile ad hoc network. The malicious node will be detected when the communication between source and destination. Two types of attackers will be found in this communication network: inside attacker, outside attacker. Onion Routing can be used to find the inside attacker and the IP address can be used to find the outside attacker. The malicious node causes the route failure or node failure when transferring the data between the source and destination. Users can quickly identify external (outside attacker) threats using the installation of an Intrusion Detection System. It takes another alternative path to send data from the source and destination. The architecture diagram shows the data transmission from source to destination. The node receives the reply message when the malicious node sends the route reply saying that it has a new sufficient route to the destination and the route reply packets having high destination sequence number it can be advertised by the source node. When the malicious node sends the RREP packet, then the route reply packet, and the threshold value has to check the destination sequence number of its previous node. If the value present in the route replay packet is greater than the threshold value of the prior node that will note its ID and consider it as malicious node. Otherwise the previous node will forward the route reply packet to its prior node and the process will continue. To Find and detect the link failure or node failure to form the cluster and to select the cluster head from transmitting the data and find the link failure path using ARS algorithm. ARS can reconfigure the failure path and to provide the secure communication between the source and destination. The link failure occurred in the order of a few minutes to hours, the short term failure occurs in the order of milliseconds it may be sufficient for dynamic resource allocation. The long term failure occurs in a few weeks or months and it can use the algorithm to recover from the failure path. ARS algorithm can be used to detect the link failure to initiate the network
reconfiguration. When detecting the link failure the ARS can accurately measure the quality of links. It can be necessary to change the network configuration to recover from the link failure.

3.2 Anonymous Routing
To develop the anonymous protocols, a common method can be used to anonymize the ad hoc on-demand routing protocols, such as AODV and DSR. For this purpose, we established the anonymous security associations between the source, destination, and every intermediate node along a route. We focus on the MANETs in adversarial environments, where the Mobile nodes initially deploy the public and group keys. We assume that there is no online security or localization service available when the network is deployed. Sender anonymity, receiver anonymity and unlinkability of the sender and receiver are the three types of anonymous communication. Sender anonymity defines that the identities of the sender should be hidden and the receiver anonymity means the identities of the receiver should be hidden. Unlinkability of sender and receiver means the identities of the sender and receiver cannot be identified by each other during the communication between the network but it identifies participation of the sender and receiver. An authenticated anonymous, secure routing (AASR) protocol used to overcome the un-linkability and unidentifiability problems in mobile ad hoc network.

3.3 Finding Inside attacker
MANETs face different security threats, i.e. attack that is carried out against them to disturb the normal performance of the networks. The black hole attack which occurs in mobile ad hoc networks. In which the routing protocol is used by a malicious node in order to present itself for having the shortest path to the destination node or to the packet, it wants to intercept and the availability of fresh routes irrespective of checking its routing table. The availability of attacker node will always reply to the route request and thus interrupt the data packet and retain it. Onion Routing and group signature can be used to find the inside attacker. It allocates key to the particular node and to insert the key to send the data send to the destination. Group signature can be used to trace the attacker and it provides more security to that particular destination and also the group signature can provide authentication. Every member in a group has the own private key it will be issued by the group manager. The document is signed by the group member to ensure that the receiver of the signed document can verified. The group manager can trace the signer identity and revoke the group keys.

3.4 Finding Outside attacker and recovering
The outside attacker can find by using IP address. The outside attackers get access from the network and send the spurious data to affect the performance of the whole network. The destination address and the active route can be detected by the malicious node. A malicious node enters in the communication network the destination is unreachable. The malicious node sends the route reply to the neighboring node. The neighboring node receives the route reply it establishes the inverse to the data of the source. The new information received by the route replay and allows the source node to update its routing table. The source node takes alternate path to send the data to the destination.

3.5 Cluster formation and cluster head selection
Nodes are working together to form a cluster, each cluster consist of the cluster head (CH). The cluster members (CM) are positioned within the transmission range of their cluster head. Cluster head control the clusters and to provide the frame work for channel access and routing allocation. Clustering provide the guarantee of the basic system performance such as throughput and delay when using the large number of nodes in the mobile ad hoc network. The networks allow the node to declare itself as a cluster head (CH). The node proclaims itself as a cluster head and it periodically notify the neighboring nodes and the cluster head propagates a cluster head hello packet. The cluster head transmission range can accept to participate in the cluster as cluster member. On the other hand, when a node is deemed to be a cluster manager, it has to wait for Cluster head hello packet. The cluster head have the bi-direction link to another cluster head. The cluster have the unique identification number at each node in the network and the cluster head selection is based on the link quality. The cluster head has a lowest ID, it change its state. Otherwise it stays in the cluster head the other node has to change its state. In this is a special case which may result in the cluster re-organization.
3.6 Find link failure by using ARS algorithm
The network monitor only provides the information about
node details and the channel capacity details collected by
the Channel Analyzer. If the link channel gets any problem,
then the node will generate error messages for informing
about failure with the use of ARS algorithm. The link
failure causes the data loss and delay in the network.
AOMDV protocol can be used to reduce the data loss.

3.7 Reconfiguration system

Fig 3: ARS System Architecture
The knowledge of route plan is done with the signal. The
channel fading was informed by the route managers. To
avoid fake reports in ARS scheme can be used to finding
the another path between the source and destination, the source
will check if the report made by the intermediated nodes and
if any false report fined means it will treat the node which
sends that report as a misbehaving node.

4. Result And Performance Analysis
By evaluating our proposed system, we have been carrying
out many sets of experiments with different types of
malicious attacks. In this paper, we present performance
results with some of these experiments as well as those
involving in malicious attacks. The existing and proposed
techniques shown in the table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Existing</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Discovery</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Route Maintains</td>
<td>Routing Table</td>
<td>Routing table</td>
</tr>
<tr>
<td>Route Update</td>
<td>No Update</td>
<td>No Update</td>
</tr>
<tr>
<td>Multiple Route</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Routing Category</td>
<td>Reactive</td>
<td>Reactive</td>
</tr>
</tbody>
</table>

Table 1: Comparison of existing and proposed System

4.1 Comparison of throughput in the presence of
different number of malicious nodes

The Figure shows a comparison among three protocols. The
number of malicious node increase the average throughput
of three protocols decreases obviously. AASR has ability to
detect the packet dropping attack, it gives better throughput
when compared to ANODR and AODV protocols.

4.2 Comparison of packet loss in the presence of
different number of malicious nodes

The Figure shows a comparison among three protocols. The
fake routing in the individual attack, due to the lack of
authentication, ANODR and AODV suffer more packet loss
then AASR. AASR achieves two percentage less loss ratio
than ANODR and AODV. A number malicious node varies
from 0 to 9.
4.3 Comparison of end-to-end delay in the presence of different number of malicious nodes

Fig: 5 Comparison of end-to-end delay in the presence of different number of malicious nodes

ANODR and AASR spend time in the route discovery security processing and the delay is much higher when compare to AODV. ANODR lunch new route discovery for the broken route it has more delay in processing the new route. AASR reduce the need of re routing, it results in less of delay compare to ANODR.

5. Conclusion

Secret communications are important for many applications in mobile ad hoc networks. AASR (Authenticated Anonymous Secure Routing) protocol is mainly used to defend the attacks in Mobile ad hoc network. In our studies, the route request packets are authenticated by using Onion routing and group signature. Onion routing with the route secret key authentication message is also used which defends the possible active attack without the introduction of node identities. Group signature can be used to legitimate the route request packets. The existing protocols are too difficult to discover the link failure or node failure in the secure communication network. In our work, the AOMDV protocol can be used to prevent the link failure in the communication network. In this paper, we prove that the AOMDV protocol increases the coverage area and to reduce the packet loss. Also prove that our proposed scheme effectively improves the network performance as compared to the existing protocols like AODV and AASR.

Reference


Author’s Profile

T. Parameswaran. T has received his B.E degree in Electronics and Communication Engineering from Velalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D from Anna University, Regional Centre Coimbatore. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, Regional Centre, Anna University, Coimbatore, India. He has published more than 10 research papers in various journals and conferences. He has organized 3 national level workshops. He is a student member of IEEE.

Dr. Palanisamy. C has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai, and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 13 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of technology, Sathyamangalam and Tamilnadu, India. He has published more than 30 research papers in various journals and conferences. He has organized more than 10 workshops and holds 2 funded projects. He is a lifetime member of ISTE. He won Best M.E thesis award at Thiagarajar College of Engineering, Madurai and best paper award titled, “A Neural Network Based Classification Model Using Fourier and Wavelet Features,” Proceedings of the 2nd Int. Conf. on Cognition and Recognition 2008, (ICCR 2008), Organized by P. E. S College of Engineering, Mandaya, Kastrnataka, India, pp. 664-670, 2008. His research interests include Data mining, image processing and mobile networks.

Sathiya Devi P is pursuing M.E Network Engineering in the Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. She received her B.E Degree in Computer Science and Engineering from Srinivasan Engineering College, Perambalur, Anna University, Chennai in 2008 to 2012. Her research interests are Ad-Hoc networking and Mobile networks.