2009 International Conference on Computer Technology and Development

A Scalable Secure Routing Protocol for MANETs

Liana Khamis Qabajeh, Dr. Miss Laiha Mat Kiah
Faculty of Computer Science and IT
University of Malaya
Kuala Lumpur, Malaysia
liana_tamimi@ppu.edu, misslaiha@um.edu.my

Mohammad Moustafa Qabajeh
Department of Electrical and Computer Engineering
IIUM
Kuala Lumpur, Malaysia
m_qabajeh@yahoo.com

Abstract—**Wireless Mobile Ad-Hoc Networks (MANETs) are becoming highly applicable in many fields. Due to MANETs special characteristics, secure routing may be one of the most difficult areas to deal with as opponents can add themselves to a MANET using the existing common routing protocols. This paper proposes a new model of routing protocol called ARANz, which is an extension of the original Authenticated Routing for Ad-Hoc Networks (ARAN). Later, we will demonstrate that apart from the authentication methods adopted from ARAN, ARANz aims to increase security, achieve robustness and solve the single point of failure and attack problems by introducing multiple Local Certificate Authority servers. We will reveal that via dealing with the network as zones and using restricted directional flooding, our new model will exhibit better scalability and performance.**

Keywords-Position-Based; Secure; Routing; Ad-Hoc Network

I. INTRODUCTION

Ad-Hoc wireless networks are self-organizing multi-hop wireless networks, where all nodes play a part in forwarding packets. Ad-Hoc networks can quickly and inexpensively be set up since they do not require any fixed infrastructure such as base stations or routers. Therefore, Ad-Hoc networks are becoming increasingly popular and highly applicable in many fields such as emergency deployments and community networking.

A key component of Ad-Hoc wireless network is an efficient routing protocol since all the nodes in the network act as routers. Ad-Hoc network routing protocols are difficult to design in general. There are two main reasons for that; the highly dynamic nature of the Ad-Hoc networks due to high mobility of the nodes, and the need to operate efficiently with limited resources such as network bandwidth, CPU processing capacity, memory and battery power of each individual node in the network. Moreover, the concept and structure of Ad-Hoc networks make them prone to be easily attacked using several techniques such as modification, impersonation, and fabrication.

Many works were done on securing Ad-Hoc routing protocols. One protocol of interest is the *Authenticated Routing for Ad-Hoc Networks (ARAN) [1]*. ARAN provides authentication of route discovery, setup, and maintenance. Main objectives of ARAN are to detect and protect against attacks from malicious nodes in a managed-open environment where no network infrastructure is pre-deployed, however it expects a small amount of prior security coordination. It requires the use of a trusted certificate authority server whose public key is known to all legitimate nodes. Before entering the Ad-Hoc network each node requests a certificate from this server. Every node that forwards a request or a reply must sign it so that the following node can check the validity of the previous one. We observed that although ARAN prevents a large number of attacks such as modification, impersonation and fabrication exploits, it based on a centralized trust hence; suffers from the compromised server problem and the single point of failure. Moreover, ARAN does not scale well in large networks since any request packet is flooded to the entire network.

In recent developments, position-based routing protocols exhibit high scalability, performance, and robustness against frequent topological changes. Position-based routing protocols use the geographical position of nodes to make routing decisions, which results in improving efficiency and performance. These protocols require that a node be able to obtain its own geographical position and the geographical position of the destination. Usually, this information is obtained via Global Positioning System (GPS) [2] and location services. Position-based routing protocols are categorized into three main groups: restricted directional flooding, greedy forwarding and hierarchical routing protocols. From observations, we note that restricted directional flooding has better performance than topology-based and other position-based routing protocols. Moreover, few works have been done to secure position-based routing.

For these reasons, it is a challenge to find a scalable, distributed and secure position-based routing protocol for Ad-Hoc networks. A new model of routing protocol, ARANz has been proposed in this work.

The rest of the paper is organized as follows. Section II presents our new protocol. We conclude our work and present our future direction in Section III.

II. PROPOSED PROTOCOL

In this section, we propose a new routing model called ARANz. The proposed protocol is called ARANz since it adopts the authentication steps used with the ARAN protocol and deals with the network as zones. ARANz, just like ARAN, uses cryptographic certificates to prevent most of the attacks against Ad-Hoc routing protocols and detect erratic behavior. However, ARANz introduces a hierarchal

978-0-7695-3892-1/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCTD.2009.179

distributed routing algorithm, which aims to improve performance of the routing protocol and distribute load by dividing the area into zones. Moreover it tries to achieve robustness and high level of security, solve the single point of failure problem and avoid single point of attack problem by distributing trust among multiple Local Certificate Authority (LCA) servers. Each zone has multiple LCAs that should collaborate with each other to issue certificates for the nodes inside that zone and work as backups of each others. If a misbehavior detection scheme presents in the network, then the security of our protocol can be improved through collaboration with this scheme.

Moreover, ARANz tries to exhibit better scalability, performance, and robustness against frequent topological changes by utilizing the concept of restricted directional flooding position-based routing protocols. Whenever a node needs to communicate with another one the former will get the latter's position through the LCAs of its zone, then the route request packet is sent using restricted directional flooding. This helps in reducing overall overhead and saving network bandwidth. Hence, the LCAs work also as position servers; and each node should inform the LCAs of its zone about its new position at a rate proportional to its speed.

ARANz consists mainly of network setup (which includes certification process, dividing the area into zones and electing the certificate authority servers), location service and route discovery and setup. All position and routing packets are authenticated end-to-end and only authorized nodes are allowed to participate at each hop between source and destination.

A. *Network Setup*

We assume N cooperative nodes in a managed-open environment. These nodes are distributed randomly in (A×A) Km^2 area and aware of their positions (equipped with GPS receivers). This area will be divided into Z zones; the area of each zone is (A×A)/Z km^2. Communication among nodes is done (mainly) using restricted directional flooding with adopting the authentication steps used with the ARAN protocol. A given node in the network is chosen to have the software needed to begin the network setup, divide the area into zones and elect the initial LCAs. This node is called the Primary Certificate Authority (PCA) server and has the private part of the network key (K_{NET-}). All the trusted nodes that will participate in the network have a private/public key pair, the public part of the network key (K_{NET+}) and a Common Key (CK) which is used for encryption and decryption of packets sent by non-PCA nodes in the network setup phase. Keys are a priori generated and exchanged through an existing relationship between PCA and each trusted node.

The PCA starts the network setup by flooding a NETwork SETup (NETSET) packet notifying the nodes about the beginning of the network setup phase. This packet is signed by K_{NET-} to enable nodes to make sure that the PCA is really the node that has sent the packet. Each node, i, upon receiving the first NETSET packet will record the IP address of the previous node, continue broadcasting the packet and reply with a Node INformation (NIN) packet to the PCA. This NIN packet contains the node's IP address (IP_i), along with the needed information to elect the LCAs. The NIN packets are encrypted using the CK. Each node upon the receipt of a NIN packet will try to decrypt it using CK to ensure that its previous node is trusted and to proceed in processing the packet; otherwise the packet is dropped. After encrypting the NIN packet, it is sent through the reverse path till reaching the PCA.

After receiving the NIN packets from all authorized nodes existing currently in the network, PCA will divide the network into multiple virtual zones and assign four LCAs for each zone (located as close as possible to the zones' edges). The details of the authentication and certification processes, dividing the area into different zones and electing the LCAs are deleted due to space restriction. The new model is shown in Fig. 1, if we suppose that the whole area is divided, for example, into nine zones.

After that, the PCA will unicast a Node ROLE message (NROLE) to each participant node. Source routing will be used to send these messages since the PCA knows the position of all the nodes in the network. These messages will enable each node to know its role in the network, i.e., LCA or normal node.

Hence, the PCA will unicast a NROLE message for each participating normal node, i, containing node's certificate ($Cert_i$), number of the zone where it is reside (j), identities and positions of LCAs in its zone, and the public key that will be used in this zone (K_{Zj+}). The node certificate ($Cert_i$) contains the IP address of i (IP_i), the public key of i (K_{i+}), a timestamp (t) of when the certificate was created, and a time (e) at which the certificate expires. These variables are concatenated and signed with the K_{NET-}. Nodes use these certificates to authenticate themselves to other nodes during the exchange of network maintenance, position, routing and data packets.

The PCA also will unicast a NROLE message for each LCA of a zone, j, containing the node's certificate, zone LCAs certificate ($Cert_{LCAZj}$), the number of that LCA in its zone, the number and coordinates of the zone it is responsible for, numbers and coordinates of this zone's 8-neighboring zones, private/public key pair that will be used in this zone, identity and position of other LCAs in this zone, identity and position of its adjacent LCA in the neighboring zone, public key of the immediate neighboring zone, and the authentication table. Moreover it will contain a list of IP addresses and public keys of authorized nodes that were not in the network during network setup; this will enable these nodes to join the network from any zone at any time.

The authentication table contains a tuple (IP_i, K_{i+}, t, e, and position) for each node, i, inside this zone. It is used to update the nodes' certificates. Also it is used upon the receipt of position request packet; LCA checks whether the destination of the route is local or external one; in order to send a position reply packet to the source or send position request packet to neighboring zones respectively.

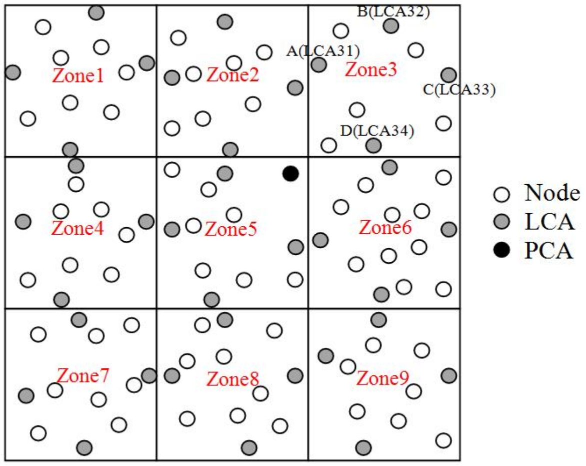

Figure 1. System modeling.

The zone LCA certificate (Cert_{LCAZ3}) binds zone's number to its public key and contains the zone number, zone public key, time stamp and Certificate expiration date. These certificates are signed by the zone private key and used by LCAs as a proof that they are LCAs of the specified zone. These Certificates are used between LCAs of different zones and between LCAs and nodes in their zones during the exchange of network maintenance and position packets.

B. *Network Maintenance*

After the network setup phase, node can update its certificate, move freely in the network, move in and out the network, become corrupted or even destroyed, etc. Since each node by the end of the network setup phase will have its node certificate, these certificates can be used to apply the authentication steps used with ARAN protocol. Hence the source of any packet will sign the packet using its private key and appends its node certificate to the packet. If the source of a packet is a LCA it will also include its zone LCA certificate within the packet to enable the destination to make sure that the LCA has a valid certificate for its zone. Each node along the path validates the previous node's signature (using the previous node's public key, which is extracted from its certificate), removes the previous node's certificate and signature, signs the original contents of the packet, and appends its own certificate.

The packets sent from the nodes to LCAs of their zones is done using restricted directional flooding, since each node within that zone know the position of these LCAs. Also communication between nodes, in the same zone or different zones, is done using restricted directional flooding (after obtaining the destination position by the source). Restricted directional flooding is also used for communications among adjacent LCAs in neighboring zones, if they are not reachable within one hop. However source routing is used to send packets among LCAs of the same zone and from the LCAs to nodes in their zones; since these LCAs know the position of all the nodes in their zone. Reply packets are sent through reverse paths of their corresponding request packets.

Many cases have been taken into consideration such as dealing with compromised, malicious and failed nodes; as well as empty zones. However they are deleted due to space limitations. The following two sub sections discuss the certifications update process and node movement to neighboring zones.

1) *Certifications Update*

All nodes in a specific zone must maintain valid certificates with the LCAs in their zone. This is done by periodically sending a Certificate REQuest (CREQ) packet to the nearest LCA. This CREQ packet is signed by node's private key and sent using restricted directional flooding. Fig. 2, shows the certificate request packets sent for updating Node's K certificate.

Each intermediate node that receives this CREQ packet verifies that it did not already processed this CREQ, records its predecessor and uses public key of predecessor (which is extracted from its certificate) to validate the signature and verify that its certificate did not expired. Then it signs the contents of the packet, appends its own certificate and broadcasts the packet to its neighbors.

The corresponding LCA upon the receipt of the first CREQ packet will communicate other LCAs in its zone to ask them whether to update this certificate or not. This is done by sending a packet to each LCA asking for Acceptance of the Certificate REQuest (ACREQ).

So a given LCA will be allowed to issue a certificate only if it received Acceptance for Certificate REPly (ACREP) packet from the majority of the LCAs of that zone. This will help in increasing the robustness and security of the protocol; if one server is failed or compromised the other three servers will still be able to update certificates of valid nodes. After receiving the required ACREP packets, the LCA will unicast a Certificate REPly (CREP) packet back along the reverse path to the source.

This LCA will also unicast a Node CERTificate (NCERT) packet to other LCAs in its zone containing the new issued certificate (to enable LCAs inside a particular zone have identical information). The LCAs also must maintain fresh node and zone LCA certificates. Hence periodically each LCA should unicast ACREQ to other LCAs in its zone. And upon the receipt of the ACREPs it will issue itself both node and zone LCA certificates.

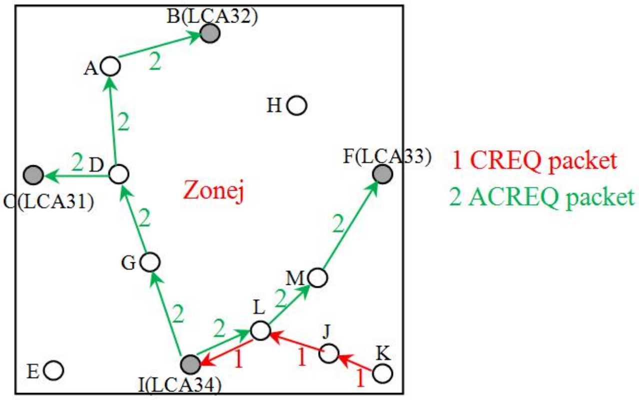

Figure 2. Node K certification update.

The following is the algorithm executed upon receiving a CREQ packet from a trusted node.

```
If (not duplicate packet) and (current node is intermediate node)
  Broadcast CREQ if closer to destination than predecessor
Else
  /* The nearest LCA */
  If (not duplicate packet) and (current node is the destination)
    {Send an ACREQ to each LCA in its zone using source routing
    No- of-available-LCAs = 4 – No-of-failed-or-compromised-LCAs
    LCAs majority= Int (No- of-available-LCAs /2) + 1
    Wait till Cert-Pre-Defined-Time-Elapsed
    If (Number-of-received-ACREP-packets >=LCAs majority)
        If (current LCA is the Source)
          Issue its self a node and LCA certificates
        Else
          {unicast CREP along the reverse path to the source of the CREQ
          unicast NCERT to other LCAs}
    } /* If the current node is the nearest LCA */
Else
  Discard the packet
```

2) *Nodes Mobility*

If a non-LCA node has moved a pre defined distance (d) from its last known position it should include its new position in the CREQ packet sent to the nearest LCA in its zone. This LCA will in turn send the node's position to other LCAs in its zone within the ACREQ packet. This will help the LCAs keep track of up-to-date positions of the nodes inside the zone and enable them to discover that a specific node has departed this zone to the neighboring one.

If the node leaves to one of the immediate 4-neighboring zones (Node movement to a D-neighboring zone is omitted due to space limitation), the LCAs of the departed zone will remove the node's information from their tables and the nearest LCA to the new zone will send a Departed NODE (DNODE) packet to its adjacent LCA. This packet indicates that this node is trusted and contains its position. Fig. 3 shows the communication done when R leaved zone number 5 to zone number 6 (moved from position P_R to P'_R). The LCA in the new zone will send a New ZONE (NZONE) packet to the departing node; containing the number and public key of the new zone, and IP addresses and positions of LCAs of that zone. This LCA also will send multiple New NODE (NNODE) packets to other LCAs in its zone telling them about the new node.

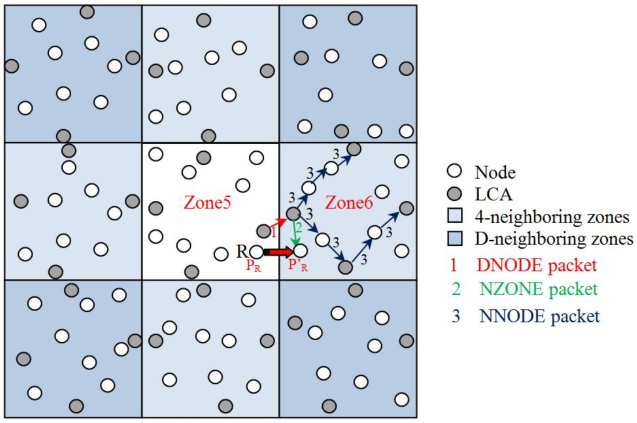

Figure 3. Movement of node R from zone 5 to a 4-neighboring zone.

If any LCA has been moved the pre defined distance (d) from its last known position, it must broadcast its position to the nodes inside its zone (including other LCAs). It also should send its position to its adjacent LCA in the neighboring zone. However, a LCA may decide to leave its zone, or its distance from the middle point of the zone side may become higher than a pre defined distance (dz). In these two cases a new LCA election is required. Upon deciding to leave its zone, LCA will send a New LCA Election (NLCAE) packet to nodes in its zone. Each node in the corresponding zone will calculate its probability by itself to reduce the load on the leaving LCA. Then each node will send its calculated probability, through reverse path, to the leaving LCA. Now the leaving LCA selects the node with the highest probability to become the new LCA. Then it broadcast a New LCA (NLCA) packet so that all nodes inside that zone know the address and position of the new LCA. This information is also sent to the adjacent LCA in the neighboring zone through a New Adjacent LCA (NALCA) packet. The leaving LCA will transfer to the new LCA the needed information (similar to that sent from PLCA to LCA nodes during network setup phase).

C. *Authenticated Location Service*

Before beginning the route discovery the source should know the destination's position. The source (S) sends a Position REQuest (PREQ) Packet to the nearest LCA in its zone using restricted directional flooding to ask the LCA about the position of the destination (D) (refer to Fig. 4).

Upon receiving the first PREQ the LCA will check whether the destination is in its zone or not. If the destination is in the same zone of the source, the destination will be found in the authentication table of the LCA. Hence the LCA will unicast a Position REPly (PREP) Packet to the source. This PREP contains the destination's position and goes back along the reverse path to source.

If the destination is in a different zone, the destination will not be found in the authentication table of the LCA. So the LCA will send multiple source routing unicast PREQ packets to other LCAs in its zone which have adjacent LCAs. Each LCA in that zone will send this PREQ to its adjacent LCA in the neighboring zone.

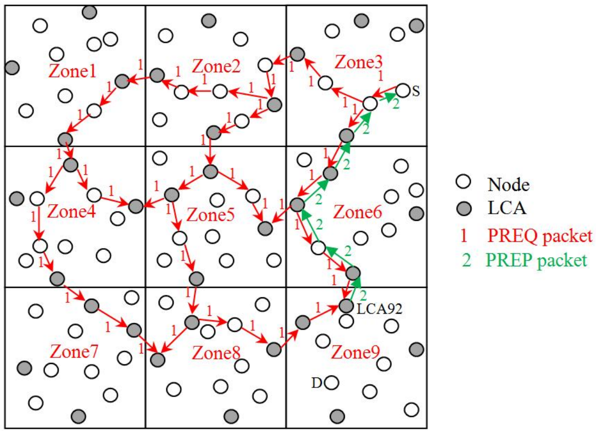

Figure 4. Authenticated location service.

Now each LCA in the neighboring zones will check if it has received the packet from other LCAs in its zone, it will drop it. Else it will unicast PREQ to the other LCAs in its zone those have adjacent LCAs in neighboring zones. These steps will be repeated until one of the LCAs (LCA92 in Fig. 4) finds the destination in its authentication table. This LCA, in turn, will unicast a PREP back along the reverse path to source. The following is the algorithm executed upon receiving a valid PREQ packet.

```
If (internal PREQ)
 /* from the source (S) to the nearest LCA in its zone */
 If (not duplicate packet) and (current node is intermediate node)
   Broadcast PREQ if closer to destination than predecessor
 Else  /* the nearest LCA */
   If (not duplicate packet) and (current node is the destination)
     If (the destination is in the same zone of the source)
       Unicast PREP back along the reverse path to S
     Else
       Use source routing to send PREQ to other LCAs
       in the current zone which have adjacent LCAs
Else    /* If (external PREQ) */
 /* between LCAs if the source and destination are in different zones */
 If (not duplicate packet) and (current node is intermediate node)
   If (Packet is sent between LCAs inside the same zone)
     Forward PREQ to the next hop in the source route
   Else    /* Packet is sent between different zones*/
     If (PREQ is not a 1 hop unicast packet)
       Broadcast PREQ if closer to destination than predecessor
 Else  /* The destination LCA */
   If (not duplicate packet) and (current node is the destination)
     {If (The packet is from the same zone)
       If (the adjacent LCA is within the transmission range of this LCA)
         Send PREQ to adjacent LCA using 1 hop unicast.
       Else
         Send PREQ to adjacent LCA using restricted directional flooding
     Else  /* adjacent zone */
         If (destination is in this zone)
           Unicast PREP along the reverse path to the source of the PREQ
         Else
           Use source routing to send PREQ to other LCAs
           in the current zone which have adjacent LCAs}
   Else
     Discard the packet
```

D. Authenticated Route Discovery, Setup and Maintenance

After getting the destination's position the source begins route instantiation to destination by sending a Route Discovery Packet (RDP). This is done using restricted directional flooding to the source's neighbors. When the destination receives the first RDP it will unicast a Route REPly (RREP) Packet back along the reverse path to the source. All the route discovery steps are done using the authentication steps used with ARAN protocol. The following is the algorithm executed upon receiving and validating a RDP Packet.

```
If (not duplicate packet) and (current node is intermediate node)
 Broadcast RDP if closer to destination than predecessor
Else
 /* destination of a RDP packet */
 If (not duplicate packet) and (current node is the destination)
   unicast RREP along the reverse path to the source of the RDP
 Else
   Discard the packet
```

ARANz is an on-demand routing protocol; nodes keep track of whether routes are active or not. When no data is received on an existing route for that route's lifetime, the route is simply deactivated. Data received on an inactive route causes nodes to generate an ERRor (ERR) packet. Nodes also use ERR packets to report links in active routes that are broken due to node movement. All ERR packets must be signed.

After finishing the route discovery and setup the source will begin sending the data to the destination. Only the control messages between nodes are subject to signing and verifying; once the route reply reaches the originator, it is guaranteed that the route found is authentic.

III. CONCLUSION AND FUTURE WORK

A new routing protocol, called ARANz, has been proposed in this work. This protocol addresses the managed-open environment where the possibility to use already established infrastructure is available. ARANz introduces a hierarchal and distributed routing algorithm, which improves performance and scalability of the routing protocol by dividing the area into zones. ARANz aims to achieve robustness, increase network security and solve the single point of failure and attack problems by introducing multiple LCAs. Our ARANz also tries to exhibit better scalability, performance, and robustness against frequent topological changes via the restricted directional flooding.

Due to large number of nodes and the large geographical area of Ad-Hoc networks a simulation tool will be used to study the performance of the new protocol. Our next tasks are to evaluate the effectiveness of the protocol in dealing with security issues. Comparisons will then be performed with the existing protocols.

REFERENCES

[1] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad Hoc Networks". *IEEE Journal On Selected Areas In Communications,* Mar. 2005, vol. 23, No. 3, pp.598-610.

[2] E. Kaplan, and C. Hegarty, 2005, "*Understanding GPS: principles and applications",* ISBN: 1580538940, 2nd Edition, Artech House, Boston, MA, USA.