Distributed Certificate Authority Under the GRID-Location Aided Routing Protocol

JiHyung Lim[1], DaeHun Nyang[1,⋆], Jeonil Kang[1],
KyungHee Lee[2], and Hyotaek Lim[3]

[1] Information Security Research Laboratory,
INHA University, Korea
{bolter, dreamx}@seclab.inha.ac.kr, nyang@inha.ac.kr
[2] Department of Electrical Engineering, University of Suwon, Korea
khlee@suwon.ac.kr
[3] DongSeo University, Korea
htlim@kowon.dongseo.ac.kr

Abstract. Ad hoc network is the network which can be considered without a pre-constructed infrastructure, and a mobile node can join the network freely. However, the participation of the mobile nodes to the ad hoc network brings up much burden of re-computation for new routes, because it leads to losing the connection frequently. Therefore, it needs authentication against the mobile nodes. To make that possible, we have two methods: single Certificate Authority(CA) and distributed CA. In the case of single CA method, the wireless network can be collapsed owing to expose the CA, but still the distributed CA method is a little safer than previous one because it needs attacks toward a lot of CAs to collapse the network. We can consider secret sharing scheme as the method that constructs the distributed CA system, but it is weak when the network size is too large. In this paper, we suggest hierarchical structure for the authentication method, and show the results of simulation.

Keywords: Ad Hoc Network Security, Authentication, Certificate Issuing.

1 Introduction

Various researches have been considered to solve the ad hoc network security problems, and most of the studies focus on how to exchange key between nodes, and how to transmit the data though secure paths[6][7]. Also, threshold cryptography has been adopted to construct the "distributed CA" by distributing private keys to several nodes[2]. In this case, public key information must be signed by at least threshold numbers of partial keys and then, they must be combined to make a valid certificate for some global public key. However, if this model is adapted, it might lead to some problems in large-scale network, because it brings up an amount of overhead to request partial certificates from whole nodes in the network.

⋆ Corresponding author.

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3983, pp. 380–387, 2006.

In this paper, we suggest an efficient method to implement distributed CA using the hierarchical grid structure. When a node participates in the network, it is issued a certificate by nodes in the smallest grid, not in the whole network. To transmit data to the other nodes, a node checks whether the target node is in its group(grid) or not. If not, the node should increase grid level to the smallest level where these two nodes reside in that same grid. It would be more efficient than certificate issuing method by the whole network because we can take advantage of locality in communication. We will describe this method in section 2 and prove the efficiency by simulation in section 3.

2 Proposed Authentication Protocol

The basic routing technique which we used in our scheme is Grid Location Service[1]. We add some processes to perform the certificate issuing function. A node needs its own public and private key pair, and has to obtain the information of the group which it is going to join in from its neighbor nodes before it participates in the network. If the nodes know the information about dealer node, they can obtain a group list and share values from a dealer node. The node should obtain signed public key information as a certificate from the nodes in its group list before it sends out some data. If the destination node does not belong to its group, the node should obtain larger group's node list for communication such that both the source and the destination should belong to the same group.

2.1 Packet Type and Share Holding Table

Some new packet types are needed for performing certificate issuing process in the existing grid location service scheme [1]. Packet types can be classified by type for obtaining group share or certificate.

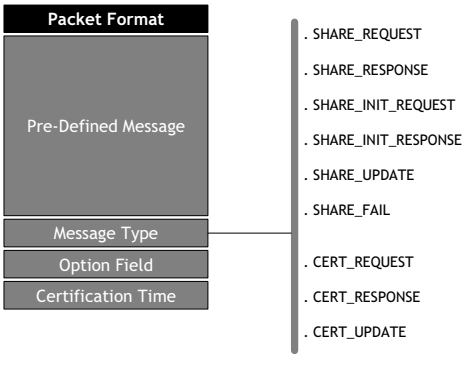


Fig. 1. Packet Format

The Packet for Obtaining Group Share

- SHARE_REQUEST: the message for requesting the information including share about its group from neighbor nodes.
- SHARE_RESPONSE: the message for responding to SHARE_REQUEST message containing Dealer ID.
- SHARE_INIT_REQUEST: the message for requesting establising a group with neighbor nodes.
- SHARE_INIT_RESPONSE: the message for responding to SHARE_INIT_REQUEST.
- SHARE_UPDATE: the message for sending the changes of a group to the group members.
- SHARE_FAIL: the message for notifying that a node has no information to SHARE_REQUEST message.

The Packet for Obtaining Certificate

- CERT_REQUEST: the message for requesting a signed message to a node's certificate from its group members.
- CERT_RESPONSE: the message for responding to CERT_REQUEST and including partially signed message.
- CERT_UPDATE: the message for notifying the update of expired certificate.

	Share Holding Table			
Item 1	GROUP-HIERARCHY	Node List	Node's Share Value	Group Establishing Time
Item 2	GROUP-HIERARCHY	Node List	Node's Share Value	Group Establishing Time
Item 3	GROUP-HIERARCHY	Node List	Node's Share Value	Group Establishing Time
...	...	...	...	...
Item n	GROUP-HIERARCHY	Node List	Node's Share Value	Group Establishing Time

Fig. 2. Share Holding Table

Share Holding Table. Every node needs the structure called "Share Holding Table" like in figure 2 for keeping secret shares of each group. "GROUP-HIERARCHY" is a group's ID that is based on x and y axis and is unique value. "Node List" contains nodes' IDs that belong to the order indicated by the value of GROUP-HIERARCHY. Each node can request a certificate from the group members, and then it can communicate to the others using that value. "Node Share Value" can be taken from the dealer node of a group, and a node uses it when the others request signed messages. "Group Establishing Time" is the time value when the owner of the table has joined in the corresponding group and received the share.

2.2 Protocol

At the beginning, a node should prepare its own public and private key pair to use it in the network. Our protocol consists of two phases. The first phase takes place when a node obtains the share value of the group, and the second phase takes place when the node obtains the certificate from the other nodes using the value. A node should obtain the certificate of the group for communicating with the other nodes, and the certificate also must be recognizable by the destination node. To do this, a node performs the following share acquisition procedure and the certificate acquisition procedure for the grid of order 1 whenever it joins the network. Also, when it sends out some data and the destination node does not belong to its group, the source node should obtain larger group's node list for communication such that both the source and the destination should belong to the same group. In the worst case, the common group might be the world grid. In the following protocol description, the dealer node takes part in the protocol, but the dealer node can be removed from the protocol because the dealer can be distributed over all the nodes if the secret sharing scheme is homomorphic.

Share Acquisition Procedure. A node should obtain the information of the group that it is going to join in before being issued a certificate. The information can be inserted into Share Holding Table of the node. The share acquisition procedure is as following :

A sender decides the order's #Order so that both sender and receiver may belong to the same grid of #Order. For obtaining the information about the group, the node broadcasts SHARE_REQUEST message to neighbor nodes. Referring the Share Holding Table, they respond with SHARE_RESPONSE if they have the information about their group, or respond with SHARE_FAIL if they do not have. If the node receives SHARE_RESPONSE message, it should register itself to its group's dealer node. And then, the node can obtain group list and share value from SHARE_UPDATE message from the dealer. If the node receives SHARE_FAIL message, it has to send SHARE_INIT_REQUEST message again for establishing a group with neighbor nodes. If a node receives SHARE_INIT_REQUEST message, it should relay that message to neighbor nodes and make the neighbor nodes send SHARE_INIT_RESPONSE message to the first issuer of SHARE_INIT_REQUEST. By sending SHARE_UPDATE to all nodes of concerned group, a dealer node should update their Node List when a new node arrives.

Certificate Acquisition Procedure. After the share acquisition procedure, a node can do certificate acquisition procedure as in the following : If a node receives the information about a group, it should obtain the certificate which is used in the group. The node sends the message including its own public key to the other nodes in the group as CERT_REQUEST message. If the other nodes receive that message, they should sign the message by their partial private key for the group and return it as CERT_RESPONSE message. If a certificate is expired after the node obtains the certificate, the node should notify neighbor nodes that the node needs new certificate by CERT_UPDATE. By sending

CERT_UPDATE, a node should update its certificate from the node of the concerned group when the time of the certificate is expired. By performing the share acquisition procedure and the certificate acquisition procedure, the sender can obtain a certificate that is verifiable by the receiver.

3 Simulation and Results

We used the discrete network simulation tool called NS-2 for our simulation and the scenarios of the simulation have two cases: non-mobility and mobility. We compared with two methods, authentication method by whole network(named "Entire") and by group network(named "Grid") in each scenario. "Grid 1" is the case when the nodes communicate in order 1. "Grid 2" is the case when the nodes communicate in order 1(50%) and order 2(50%). "Grid 3" is the case when the nodes communicate in order 1(30%), order 2(30%), and order 3(40%). "Random" is the case when the nodes randomly communicate in all orders.

We performed this simulation using 100 mobile nodes for 400 seconds.

3.1 Non-mobility Case

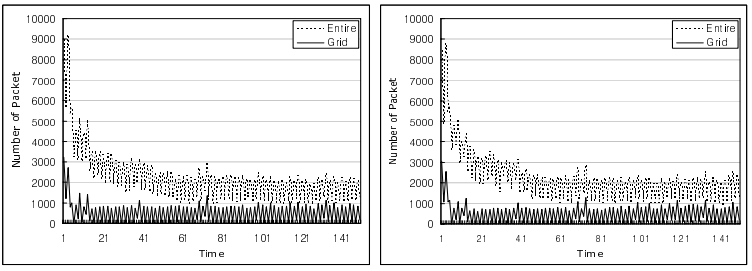
Total Control Packet. The amount of total packets is shown in figure 3. A lot of control packets for issuing a certificate are required to issue a certificate in the beginning of Entire case because share acquisition and certificate acquisition procedures are required before the first transmission of data. On the other hand, small numbers of packets in Grid method are required because only the nodes in the grid that covers both sender and receiver involve in the certificate issuing procedure. Also, Grid method consumes shorter time than Entire method before transmitting data after certificate issuing.

Control Packets for Certificate. The amount of control packets for issuing certificate per unit time (second) is shown in figure 4. After a certificate issuing is completed in the beginning, the nodes keep generating the packets for updating certificates. Grid method requires short time, about $5 \sim 6$ seconds, but the Entire method requires longer time about $30 \sim 40$ seconds for initial certificate issuing.

Accumulated Total Packets. Figure 5 shows the number of accumulated total control packets in the time. We could notice the big difference in the amount of packets used in Grid and Entire method from the figure.

3.2 Mobility Case

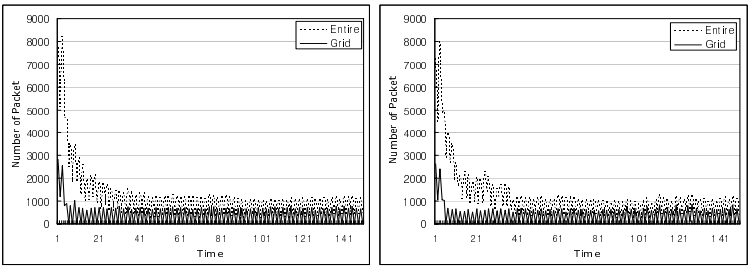
Threr is no big difference between the Non-mobility and mobility cases, even though the result was different from our expectation. This unexpectation might be because of following reasons : nodes generate a lot of packets to be issued a certificate at the beginning because they have no information about the groups, but a lot of nodes which obtain the information can serve it to the other nodes. Therefore, we might be able to say that the mobility of nodes hardly have an influence on the amount of the total control packets of all nodes.



(a) Grid 1 vs Entire (b) Grid 2 vs Entire

(c) Grid 3 vs Entire (d) Grid Random vs Entire

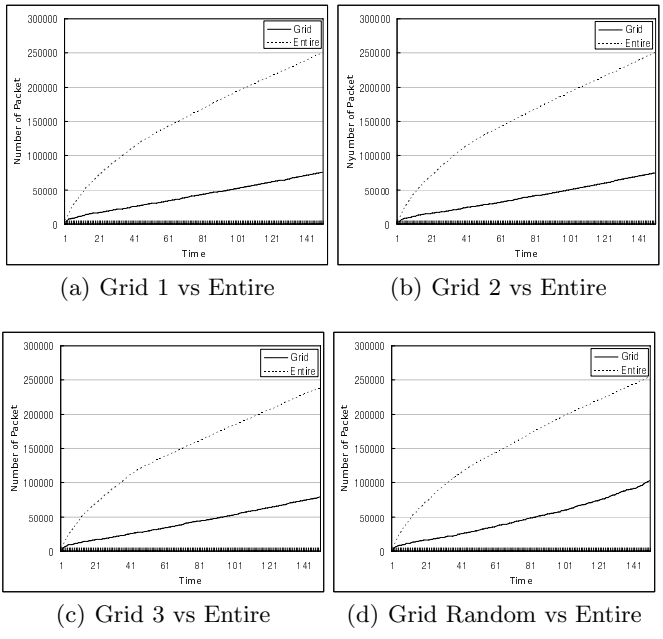
Fig. 3. Total Control Packets



(a) Grid 1 vs Entire (b) Grid 2 vs Entire

(c) Grid 3 vs Entire (d) Grid Random vs Entire

Fig. 4. Control Packets for issuing a certificate



(a) Grid 1 vs Entire (b) Grid 2 vs Entire

(c) Grid 3 vs Entire (d) Grid Random vs Entire

Fig. 5. Accumulated Total Packet

3.3 Certificate Issuing Latency

Certificate Issuing latency is the time to be measured for taking certificate before data transmission. It is from the moment when a node requests a group share till a node obtains messages signed by partial private keys from over 50% of nodes that have received requesting messages. This result shown in figure 6 seems to be based on two reasons. At first, it has difference because the time for a node to obtain a group share is faster than the time required to obtain a certificate. Secondly, if dealer node is changed while a node is obtaining a certificate, the node should obtain a new group share from changed dealer node and it should perform the certificate issuing procedure again.

4 Conclusion

In this paper, we discussed how to construct a distributed CA efficiently using grid location service scheme. Existing the secret sharing methods can construct a distributed CA using a partial private key in ad hoc network, but it has a problem in that it costs long delay for issuing a certificate. It brings up the result that it wastes network resources, because a node should involve in certificate issuing procedure even though it does not want to communicate with others.

We solved that problem using a hierarchical grid for constructing a distributed CA. Using our scheme, delay and traffic can be shorter and less than the entire

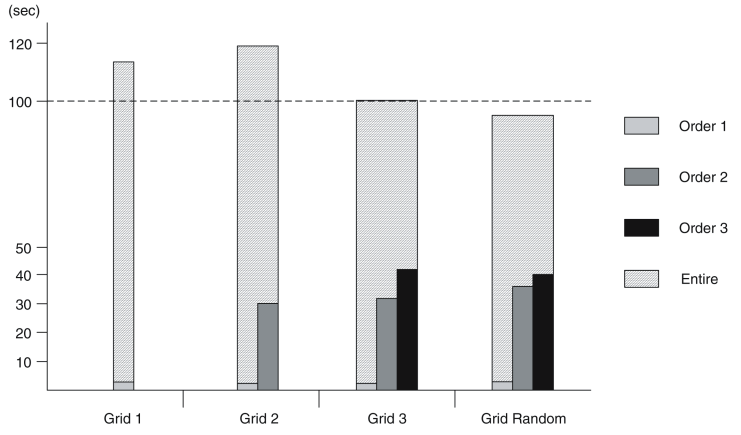


Fig. 6. Average certificate issuing latency of Entire and Grid method(unit: *sec*)

method in the beginning of the network operation. We expect that our scheme can be applied as a certificate issuing framework for other different wireless network systems.

References

1. Jinyang Li: A Scalable Location Service for Geographic Ad Hoc Routing, 6th ACM International Conference on Mobile computing and Networking (MobiCom'00), pp.120-130, Aug. 2000
2. L. Zhou and Z.J. Haas: Securing Ad Hoc Networks, IEEE Network Magazine, Vol. 13, no. 6, Nov. 1999
3. Jiejun Kong: Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks, IEEE 9th International Conference on Network Protocols (ICNP'01), pp.251-260, 2001
4. Shamir A. : How to Share a Secret, Communication of the ACM, pp.612-613, Nov. 1979
5. T.P. Pedersen : A threshold cryptosystem without a trusted party, Advances in Cryptology, Proceedings of the CRYPTO'91, pp. 522-526, 1991
6. Stephen Carter and Alec Yasinsac, Secure Position Aided Ad hoc Routing Protocol, Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02) Nov 3-4, 2002
7. Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun, The Quest for Security in Mobile Ad Hoc Networks, Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing 2001, 2001