Proceedings of the International Multiconference on Computer Science and Information Technology pp. 445–451
ISSN 1896-7094


# Public Key Management Scheme with Certificate Management Node for Wireless Ad Hoc Networks

Shunsuke Funabiki[1], Takamasa Isohara[1], Yuko Kitada, Keisuke Takemori[2], and Iwao Sasase[1]

[1] Department of Information and Computer Science, Keio University,
{funabiki,isohara,sasase}@sasase.ics.keio.ac.jp
[2] KDDI R&D Laboratories,
takemori@kddilabs.jp

**Abstract.** An authentication technique is an important issue for a wireless ad hoc network that is composed with unknown nodes. The self-organized public key management scheme that each node creates and manages certificates by itself has been proposed for the network that does not connect to the Internet with a certificate authority. However, it needs large time and loads heavy traffic to collect all certificates in the network. In this paper, we propose public key management scheme with repository management node that collects certificates of each node in its power range. This proposed scheme consists of selecting certificate management node (CMN) and clustering techniques. It can reduce the time to collect certificates from the CMN when normal nodes access to the CMN. Furthermore, our proposed scheme can reduce memory and traffic loads because normal nodes neither have all certificates nor exchange repositories each other. By a computer simulation, we evaluate average traffic and an amount of memory consumption and show that the proposed scheme can reduce the both of them than conventional schemes.

**Key words:** Wireless Ad Hoc Network, PKI, Certificate Chain,

## 1 Introduction

Recently, authentication techniques in ad hoc network have been paid more attention, where many nodes relay the packet concertedly and unknowing nodes come in communication. Public Key Infrastructure (PKI) is a main technique of authentication in the Internet. In PKI, Certificate Authority (CA) publishes public key certificates in order to assure the validity of private key that is a pairs of public key made by each node [1]. Hence, CA works as third trusted party. In the case of wireless ad hoc networks, it is not able to use CA, since wireless ad hoc networks does not have connecting points to the Internet. A self-organized public key management system in which each node publishes certificates independently and manages them at its repository has been proposed as the scheme each node manages public key certificates by itself [2]. In this scheme, each node stores the information of repositories, constructs certificate chains, and authenticates each other by exchanging certificates in its power range periodically. But this scheme has the problem that it has long time to collect certificates, large traffic to collect certificates, and large amount of memory to manage certificates, because each node collects all certificates in entire network.

In this paper, we propose a public key management scheme with Certificate Management Node (CMN) for wireless ad hoc networks in which CMN manages in stead of repositories in ad hoc network in order to solve these problems. CMN is selected by using a clustering technique in order to manage certificates issued by nodes in one hop. We will decide that the node which is not CMN is "Normal Node" (NN). In our proposed system, time to collect information about certificates can be reduced in comparison with the conventional scheme, because collecting certificates and managing Certificate Revocation List (CRL) are completed only by transmitting certificates and information of revocation from NNs to CMN. Since exchanging repositories is not necessary, traffic can be reduced compared with the conventional scheme. Amount of memory of a NN for constructing the certificate repository is proportional to number of certificates issued by itself. As multiple CMNs share all certificates in entire network, amount of memory of CMN is reduced in proportion to number of CMNs. By a computer simulation, we obtain traffic of network and amount of memory necessary for managing certificates. In the result, we show our proposed scheme is effective in wireless ad hoc network. This paper is organized as follows. Section 2 discusses the conventional self-organized public key management and problem of its system and section 3 describes the proposed scheme. Section 4 details a performance evaluation of the proposed scheme and section 5 describes a conclusion.

## 2 Conventional Self-organized Public Key Management

[2] shows a self-organized public key management system. In this scheme, certificate chain that shows relation of nodes is established. Fig. 1 shows establishment of certificate chain. Circle 1 to circle 7 indicates nodes and they trust in a direction of arrowed line. In Fig. 1, node 1 trusts node 2. In a similar fashion, node 2, node 3 and node 4 trust other node. Then, a certificate chain is established between node 1 and node 4. These authenticities are assured by public key certificates, and the certificate from node 1 to node 2 includes a public key of node 2 and a signature of node 1. First each node issues a certificate to a public key of reliable node independently, second it collects all certificates in entire network, third it makes repository, fourth it establishes a certificate chain to a destination node, and finally it authenticates a destination node. Each node collects all certificates in entire network by exchanging repositories the nodes in its power range periodically while moving. To manage expired certificate, each node makes CRL to describe invalid certificates. Each node verifies the effectiveness of the certificate and updates CRL by regularly inquiring the node that issued the certificate in order to keep information in CRL latest constantly.

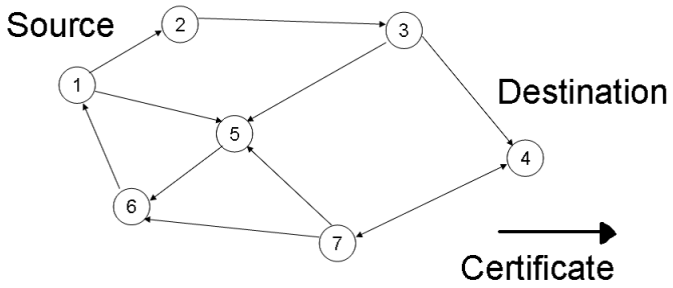


**Fig. 1.** Establishment of certificate chain.

In the conventional Scheme, it takes large time to collect certificates of entire network. For example, in an ad hoc network which is built from 100 nodes and 600 certificates, it is reported that the certificate exchange's convergence time is almost 10,000 seconds when a certificate exchange's interval is 60 seconds[2]D It is necessary to inquire the node for the effectiveness of certificates that compose a certificate chain at the time of authentication because of the time lag until completing the collection. If the number of nodes in the network is large, the size of the repository increases in all nodes because the number of certificates that should be managed becomes huge. In general, it is preferable that amount of memory for storing the certificate is little because amount of memory of a node is limited for a wireless ad hoc network where simple nodes get together. In addition, there is a problem that traffic in the network increases by exchanging repository with other node periodically. The increase of traffic causes congestion of the network and loss of data by the packet collision.

## 3 Proposed Public Key Management Scheme with Repository Management Nodes

In this paper, we propose the distributed key management infrastructure. It consists of setting CMN that manages certificates instead of each node and implementing clustering to make a relationship between CMN and NN. We explain detail as follows.

### 3.1 Architecture of Proposed Scheme

Fig. 2 shows concept of CMN. Hereinafter, a node that authenticates other node is called "Master node" and a destination node that is authenticated by Master node is called "Slave node". Each node issues a public key certificate of a reliable node and consigns the management of the certificate to CMN. Thus, CMN works as a repository of the neighborhood of node. When the authentication demand is generated, Master node receives certificates necessary to form a certificate chain from CMN. Details is described as follows.

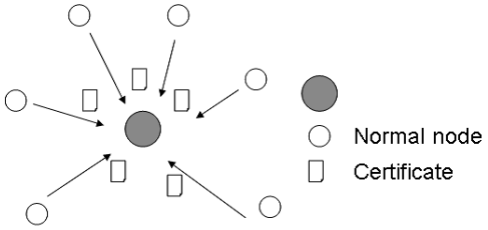


**Fig. 2.** Concept of certificate management node.

### 3.2 Selecting method of CMN

We explain the method of selecting CMN described in A-(2). An ad hoc network in the proposal method is assumed to use the OLSR(Optimized Link State Routing) protocol [4] to reduce traffic at flooding. In the OLSR protocol, each node has the Willingness value that is the value to which show its own easiness to the relay node that retransmits information at flooding. It is scored in the range from 0 to 7 where high value means easiness to become a relay node. It is easy to collect certificate since transmission is easy to be done more through a node that is easy to become relay node by neighborhood of node. Selecting CMN is judged based on the value of Willingness to raise the collection efficiency of certificate, and a node that is the center of routing takes the initiative in becoming CMN. Selecting method of CMN is shown below.

(1) Each node broadcasts to all nodes in the power range of one hop own Willingness value $will_i$.

(2) Each node compares $will_i$ received from the neighborhood of nodes with own Willingness value. When its Willingness value is the highest in the neighborhood of nodes, it judges that it should become the center of routing and runs for CMN. If two or more nodes have same Willingness value, priority is given to the node with an early candidacy.

### 3.3 Clustering

If the only one CMN exists, the certificates on the entire network are gathered by the one CMN and the amount of memory of CMN becomes huge. Moreover, in the viewpoint of traffic, congestion and the packet loss occur because of the access concentration. Therefore, we introduce two or more CMNs to manage to collect certificates. In this case, the process of grouping nodes "clustering" that decide the relation between NN and CMN should be considered. Here, we name this process "clustering" Fig. 3 shows a structure of cluster. The cluster is composed of CMN and NN that exists in the power range of CMN.

**Initialization of cluster** The procedure of initialization of cluster from the state that no relation between CMN and NN is decided is shown below.

(1) The node that runs for CMN broadcast of candidacy information with its identifier $ID_i^{manage}$ to the nodes within the power range.

(2) The priority of candidacy to CMN priority is given to an early candidacy, and candidate that received candidacy information of other node belongs to its cluster without running. When a node cannot receive candidacy information, the node judges that the node that runs in its power range doesn't exist and runs voluntarily. Even if other candidacy information is received later, the node that belongs to the cluster disregards it so that the cluster should not overlap. Each node preserves received $ID_i^{manage}$ as information of CMN of the cluster that it belongs. The cluster is formed by the above-mentioned procedure.

(3) The CMN decided by candidacy announces by flooding the information that it is CMN with its identifier $ID_i^{manage}$ to all nodes in the network besides candidacy information. Flooding is done by MPR(Multiple Point Relay) flooding of the OLSR protocol, because it is an effective method that can minimizes the traffic. By this procedure, each node knows all CMNs and makes the CMN lists.

(4) After the cluster is formed, each node passes issued certificate and its identifier $ID_i$ to the CMN of the belonging cluster.

**Restructuring of cluster** The position of the node frequently changes in wireless ad hoc network. Therefore, it is necessary to change the CMN and the cluster, and to restructure the best formed cluster

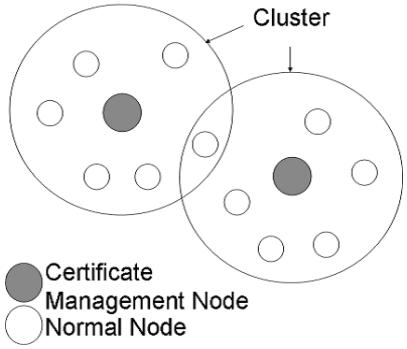


**Fig. 3.** Structure of the cluster.

in the following two kinds of situations. The Willingness value doesn't change even when the arrangement situation of the node changes.

Pattern 1: The case that CMN comes off from the power range of NN

When CMN and NN don't exist in the power range by moving of each other, NN should change the belonging cluster. The NN inquires the CMN when authenticating, and when it is not possible to communicate at this time, detects that the CMN came off from its power range. The NN broadcasts the message that it has been isolated in order to search for the existence of the cluster that it can belong newly. When other CMN exists in the power range and receives information of isolation, CMN replies the message that CMN can accept to the NN. When the NN receives the message of the CMN, the NN belongs to its cluster. The NN which belongs to new cluster sends own identifier $ID_i$ to the CMN as well as an initialization of cluster. Then, the NN passes all certificates it has. When any CMNs do not exist in the power range and the message that the NN can be accepted doesn't return, the isolated NN itself runs for the CMN. The NN that runs for the CMN broadcasts candidacy information in the power range as well as the procedure of an initial clustering, and isolated NN makes to belong to own cluster. When a NN registers the certificates in another CMN again, the CMN detects that the NN had come off from the power range by communicating with other CMN accepted re-registration communicates mutually. Then, the CMN deletes the identifier of the NN that comes off in the power range and the certificates issued by corresponding NN.

Pattern2: The case that CMN is overcrowded

When the CMN approaches to other CMN and the range of cluster overlaps each other greatly, one of clusters is dismantled because the number of NNs that belong to one cluster decreases and the management of the certificate becomes inefficiency. When it is understood that other CMNs exist in the power range of the CMN, the CMN exchanges information of Willingness value mutually, and the CMN with low Willingness value becomes NN and dismantles its cluster. CMN to which the dismantlement of the cluster was decided notifies the nodes that belongs to its cluster dismantlement, annuls the managed certificates and the identifier of the belonging node, and becomes a NN that belongs to the cluster of the other CMN. At this time, the node becoming a NN broadcasts the message that it has not been CMN with identifier $ID_i^{manage}$ to the node in the network as well as the time that a node became CMN The NN isolated by dismantlement restructures a cluster with the procedure for describing in pattern 1. When the willingness value of the CMN is the same, one with an early notification of the message of dismantlement is given priority and dismantled. When the message cannot be received by the hidden terminal problem, the notification that presses the retransmission of the message after the fixed time passes is done, and the communication is tried again.

### 3.4 Authentication

Fig. 4 shows the process of authentication. Suppose node 1 is Master node and node 7 is Slave node.

(1) Node 1 sends identifier of Master node and Slave node ($ID_1$,$ID_7$) to CMN 13 whose cluster is the node 1 belonging cluster, and inquires the certificate.

(2) When CMN 13 searches for the certificate registered in its repository and confirms that it is not able to construct a certificate chain with its certificate alone, it is inquired of other CMNs based on CMN list it made. The inquiry is done once according to the CMN list by turns via two or more nodes. Inquiry is done in order of 14 and 15 as shown in Figure 4.

(3) CMN 14 replies to CMN 13 which is the transmission origin all certificates stored in its repository after receiving the inquiry. After that, CMN 13 searches for the certificate whether a certificate chain from 1 to 7 can be constructed again together with its certificate. Next, when it is confirmed not to be able to construct a certificate chain, CMN 13 is inquired of CMN 15. This work is continued until a certificate chain can be constructed.

(4) CMN 15 replies to CMN 13 which is the transmission origin all certificates stored in its repository after receiving the inquiry. After CMN 13 received the certificates, its adds the certificate from CMN 14 to its certificates and searches for the certificate to construct a certificate chain from 1 to 7 again. As a result, since it is understood to be able to construct a certificate chain of (1234567), certificates necessary for the authentication is sent to node 1.

(5) Node 1 authenticates node 7 that is Slave node by the received certificate. After authentication succeeds, Master node and CMN delete the received certificates in consideration of memory consumption of the node. When a certificate chain can't be constructed even if all certificates in the network are collected, CMN tells Master node that it is impossible to authenticate.

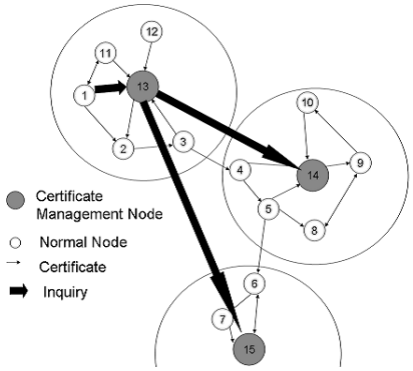


**Fig. 4.** Process of authentication.

### 3.5 Revocation of certificate

This chapter explains revocation of certificate. When the certificate is necessary to revoke by losing the private key for instance, each node sends information of certificate revocation to CMN. After receiving information, CMN annuls the certificate that corresponds to information of revocation and always keeps the latest state of the certificates. Therefore, in the authentication processing in the proposed scheme, it is needless to verify the effectiveness of the certificate and to demand CRL since the certificate that each node is inquired of the CMN and obtained is always the latest.

## 4 Performance Evaluation

To verify the effectiveness of the proposed scheme, we evaluate an amount of the memory and traffic in entire networks.

### 4.1 Time to collect certificate

In the conventional scheme, it takes large time to collect all certificates in the network by repeating exchange of the repository with neighbor node. On the other hand, in our proposed scheme, collection of certificates is achieved only by transmitting the certificate to CMN, and time to collect certificate can be reduced because each node must not individually execute the repository exchange that is necessary in the conventional scheme.

### 4.2 An Amount of memory

Fig. 5 shows an amount of memory for certificate repository. X axis shows the number of total nodes and y axis shows amount of memory. The power range of a node is 100m and the range of simulation is square

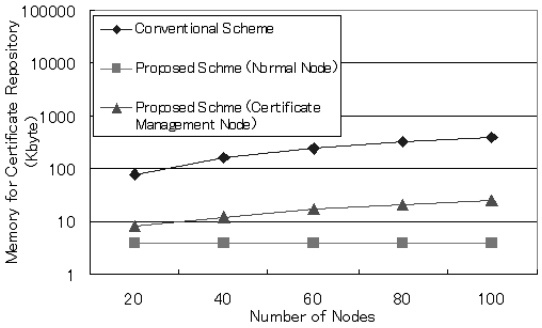


**Fig. 5.** an amount of memory for certificate repository.

of 500m 500m. The movement of the node uses random walk model that a node decides coordinates within the range at random as a destination, moves at a constant speed aiming at the destination, and sets new destination after it arrives. An amount of memory that a NN uses is only size of the certificate it issued because only the CMNs manage the certificate. Moreover, an amount of memory that CMN uses is also reduced more than one of conventional scheme because the CMNs manage the certificate on entire network by the plural allotting. For instance, when the number of all nodes is 100, about 16 CMNs are selected and the memory usage of each CMN becomes 1/16 of the conventional scheme that each node collects all certificates. The difference of an amount of the use memory between the proposed scheme and the conventional scheme grows by increasing of the number of nodes in the network. Therefore, the proposed scheme is more effective as the density of node becomes higher.

### 4.3 Traffic

Fig.6 shows traffic in network to manage certificate. The average moving speed of each node is assumed to be 10m/s, and the simulation time is assumed to be 1000 seconds. In proposed scheme, traffic to restructure cluster that arise from movement of node is about 2GByte in the case of 100 nodes and occupies 3/4 of entire traffic, but it is reduced more compared with the conventional scheme, because the confirmation of revoked certificate and repository exchange on regular to collect certificate are unnecessary. Moreover, traffic of the proposed scheme increases linearly when the number of nodes increases, but traffic of the conventional scheme increases in exponential because the node that exchange repositories at a time increases. Therefore, the proposed scheme is more effective as the density of node becomes higher. Next, the transmission by the re-composition of the cluster that depends on the moving speed of node is generated in the proposal method. Then, Fig. 7 shows evaluation result of traffic in network for varied speed of nodes when the number of all nodes is 100 and the average speed of each node is changed. When the average movement speed of each node is slow, traffic to manage certificate@decreases because the frequency of restructuring cluster decreases. That is, the proposed scheme in more effective when the passing speed of each node is slow.

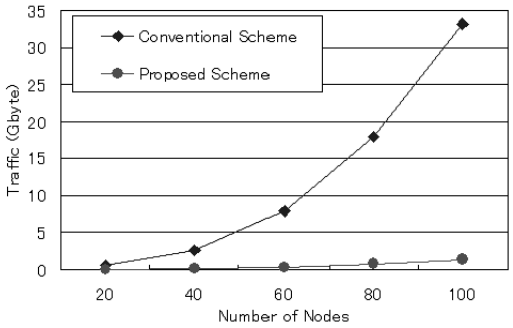


**Fig. 6.** traffic in network to manage certificate.

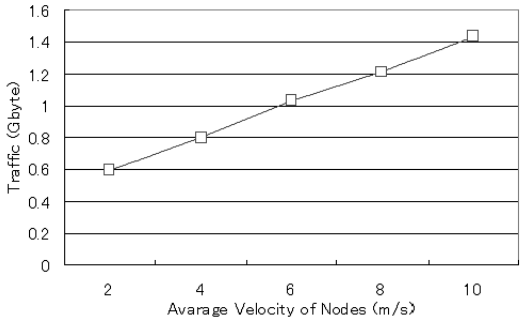


**Fig. 7.** Traffic in network for varied velocity of nodes.

## 5 Conclusion

We have proposed a scheme to manage public key certificate in a wireless ad hoc networks that is independent of the Internet. In our proposed scheme, first CMN is selected from the node in the network, second it collects certificates issued by the neighborhood of nodes, and finally it manages them instead of repository. To make a relationship between CMN and NN, our scheme introduces a technique of grouping which is called "clustering".

In our proposed system, time to collect information about certificates can be reduced in comparison with the conventional scheme, because collecting certificates and managing Certificate Revocation List (CRL) are completed only by transmitting certificates and information of revocation from NNs to CMNs. Moreover, the collection time of the certificate can be shortened. By the computer simulation, we evaluate an amount of memory used to hold the certificates and traffic in entire network and show that both can be reduced more than the conventional scheme. For an amount of memory, it is shown that the size of NN is as large as four certificates, and the size of CMN is 1/16 of the conventional scheme where one node issue four certificates on average, the area of simulation field is square of 500m 500m, the power range of a node is 100m, and the number of all nodes are 100. For traffic, it is shown that traffic of proposed scheme is 1/10 of conventional scheme in the case that the number of all nodes is 40 and is 1/20 in the case that the number of all nodes is 100. We show that traffic decreases especially when the passing speed of each node is slow because the frequency in which clustering was restructured decreased. Therefore, it is shown that the difference between the proposed scheme and the conventional scheme for an amount of memory and traffic is getting greater and greater if the number of nodes in network grows. Thus, the proposed scheme is more effective when the density of node becomes higher. Moreover, for the moving speed of node, we show that proposed scheme is more effective when the speed of each node becomes slower.

## References

1. IETF: nternet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC3280C, April 2002.
2. Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux: *Self-organized public-key management for mobile ad hoc networks,* IEEE Transactions on Mobile Computing, Vol. **2**, No. 1, January-March 2003, pp. 52–64.
3. Yuko Kitada, Yutaka Arakawa, Keisuke Takemori, Akira Watanabe, Iwao Sasase: *On Demand Distributed Public Key Management Using Routing Information for Wireless Ad Hoc Networks,* IEICE D-I Vol. J88-D-I, No. 10, pp. 1571–1573.
4. P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, and T. Clausen: *Optimized link state routing protocol for ad hoc networks,* IEEE International, 28–30 Dec. 2001 pp. 62–68.