On Demand Distributed Public Key Management without Considering Routing Tables for Wireless Ad Hoc Networks

Yuko Kitada † Keisuke Takemori ‡ Akira Watanabe §
Iwao Sasase †
†Dept. of Info & Computer Science,Keio University
Yokohama 223-8522, Japan
{yuko,sasase}@sasase.ics.keio.ac.jp

‡KDDI R&D Laboratories Inc.
Saitama, 356-8502 Japan
takemori@kddilabs.jp

§Dept. of Info & Computer Science,Meijo University
Nagoya, 1–501, Japan
wtnbakr@ccmfs.meijo-u.ac.jp

Abstract

A wireless ad hoc network that has no connection to the Internet can not use a Public Key Infrastructure(PKI). Although an on demand distributed public key management to construct the PKI has been proposed, it cannot work without considering routing tables, since nodes broadcast a packet which contains routing tables. In this paper, we propose an on demand distributed public key management which can separate the routing and authentication layers. In the proposed scheme, each node sends a packet which does not contain routing tables by unicasting. The proposed scheme can be applied to various communication protocols and simple terminals because the scheme does not need to consider routing tables in the authentication layer. By a computer simulation, we evaluate average traffic and show the adaptive flexibility of the proposed scheme in the ad hoc network.

1 Introduction

Public Key Infrastructure (PKI) [1] is recognized as one of the most effective mechanism for providing fundamental security services including authentication, confidentiality and integrity of information. However, it is unclear whether such approaches can be extended or not to a wireless ad hoc network [2]-[5] which does not have connecting points to the Internet. The wireless ad hoc network that has no connection to the Internet is difficult to construct PKI, since this network does not have any fixed or stationary infrastructure. In order to construct the PKI, an on demand distributed public key management has been examined[6]. In the scheme, in order to collect certificates necessary for forming the certificate chain efficiently, the ASNS(Ad hoc Simultaneous Nodes Search) protocol has been proposed. In the ASNS, by broadcasting a search packet which contains routing table information, all nodes necessary for forming the certificate chain can take part in the construction of the certificate chain. However, the scheme cannot work without considering routing table in the authentication layer. Therefore, the method to separate the routing and authentication layers should be considered to give expandability to the on demand distributed management.

In this paper, we propose an on demand distributed public key management which can separate the routing and authentication layers. The process in authentication layer of each node is only to designate trusted nodes. On the other hand, the process in the routing layer is to send a search packet which does not contain routing table information. In the proposed scheme, each node can send the search packet to all nodes necessary for forming the certificate chain by unicasting. The proposed scheme can be applied to various communication protocols and simple terminals because the scheme does not need to consider the routing tables in the process of the authentication layer. By a computer simulation, we evaluate average traffic, and show the adaptive flexibility of

the proposed system in the ad hoc network.

2 Table Consideration Type

Here, we call the on demand distributed management which uses routing tables in the authentication layer 'table consideration type'. On the other hand, we call the proposed scheme 'table independence type'. Here, there is a directed edge from vertex 1 to vertex 2 if there is the certificate signed with the private key of node 1 that binds the node 2's public key to an identity. The certificate is denoted as '1 → 2'. A certificate chain from node 1 to node 4 is represented by a directed path from vertex 1 to vertex 4 in the certificate graph. Also, a source node that requests to authenticate is called a 'Request node' and a destination node that is authenticated by the Request node is called an 'Authenticated node'. And a node that is trusted by other node is called a 'Trusted node'. Moreover, certificates that are necessary for forming the certificate chain are called 'Certificates of the certificate chain'. In this section, we explain a mechanism of the ASNS[6].

2.1 Initial Phase of Authentication

Step 1) Creation of Key Pairs

The public key and the corresponding private key of each node are created locally by the node itself.

Step 2) Issuing and Storing of Public key Certificates

How to issue public key certificates is the same as the conventional system. In the ASNS system, a node holds in her repository only the certificates that other nodes issue to her.

Step 3) Certificate Exchange

The exchange process of the repository information is unnecessary.

2.2 Creation of a Certificate Chain

2.2.1 Assumed Ad Hoc Routing Protocol

As a kind of the routing protocols in the ad hoc network, a proactive type protocol[9]-[12], in which all nodes always hold their own routing tables, is used. We apply the proactive type in ad hoc routing protocols by using the part of routing table information. The nodes of this protocol collect routing table information by exchanging the routing information periodically. In order that the node which is not the neighbor of the Request node can receive the request packet, the ASNS protocol adds the part of the routing table information to the request packet.

2.2.2 Search Packet

Fig.1 shows a content of a search packet and a routing table. The following information fields are added to the request packet.

- Authnode: Request node field. This denotes an identification (ID) of the node who authenticates other nodes.
- Authednode: Authenticated node field. This denotes an ID of the node who is authenticated finally.

An Authnode and an Authednode field are added to make nodes know both an Authnode and an Authenticated node. A hyphen "—" in the table denotes that the destination node is in the power range. Among the routing table information, the information corresponding to the Trusted node is added to the search packet, since nodes which are not in the power range can take part in the certificate chain.

2.2.3 Construction of Approach Path

Fig.2 shows an authentication model in the table consideration type. A table in Fig.2 shows a certificate repository. In this figure, the certificate is denoted as '1 → 2'. As shown in Fig.2(1), all the nodes in the neighborhood of the node 1 can receive the search packet when the node 1 sends the search packet by broadcasting. ' × ' mark on the vertices shows that the node ignores the search packet.

2.2.4 Behavior of Trusted Nodes and Relay Nodes

The Trusted node, which does not trust the Authenticated node, adds an own certificate to the search packet. Then, the Trusted node rewrites the table information of the search packet to the information of the nodes that it trusts. Finally, the Trusted node sends the search packet to its neighboring node by broadcasting as shown in Fig.2(2). On the contrary, the Trusted node which trusts the Authenticated node adds an own certificate to the search packet and sends it to the Authenticated node by unicasting as shown in Fig.2(4).

A node which is denoted in the next hop of the search packet is called 'Relay node'. The Relay node rewrites the routing table information of the search packet to the information of a node which the node tries to relay. Then the relay node sends the search packet to its neighboring nodes by broadcasting. Therefore, in Fig.2(3), the search packet can reach to the Trusted node 2 which is not the neighbor of the node 1.

2.2.5 Construction of Return Path

The Authenticated node sends a reply packet which contains all certificates that form the certificate chain to the Request node by unicasting as shown in Fig.2(5). By receiving this reply packet,

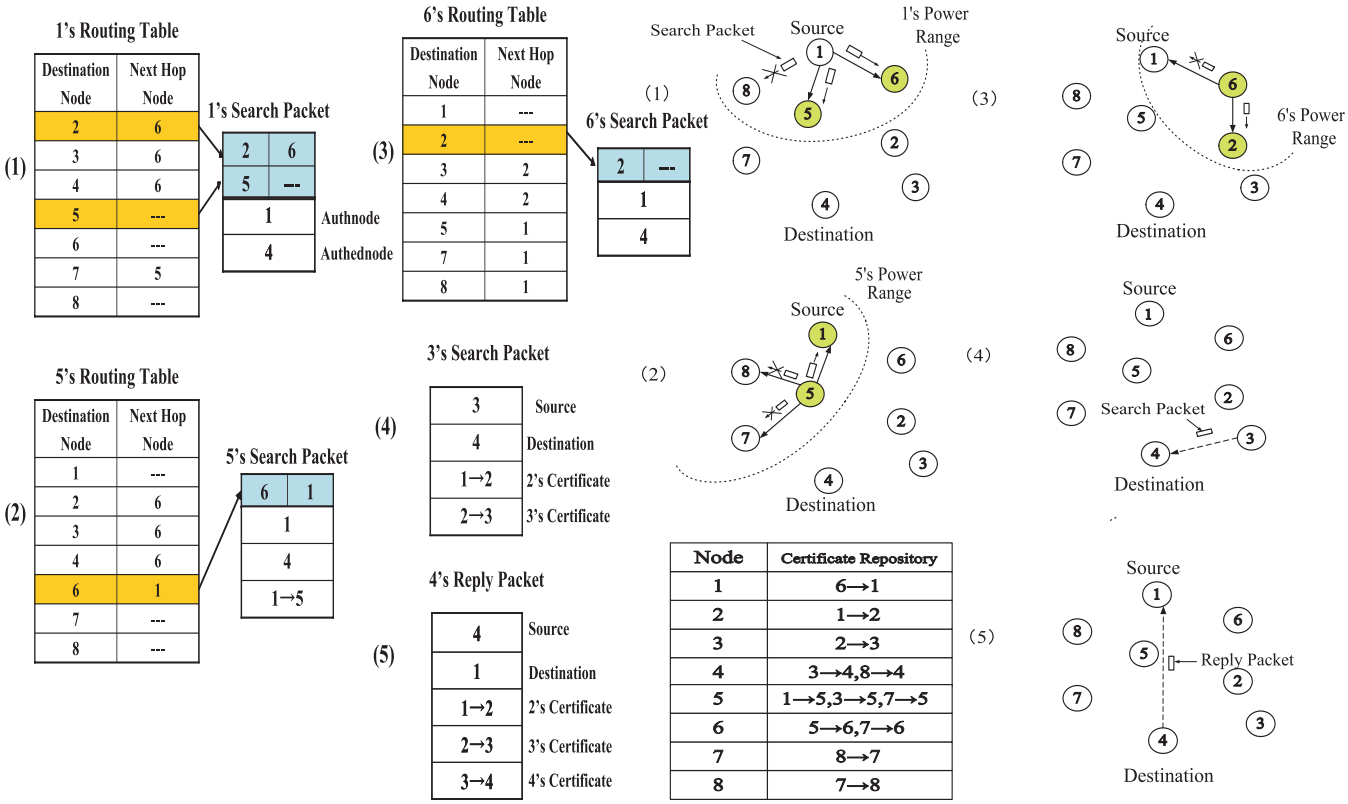

Figure 1: Content of a search packet and a routing table in the table consideration type.

Figure 2: Authentication model in the table consideration type.

the node 1 can get all of the certificates of the certificate chain.

2.3 Problems of Table Consideration Type

The table consideration type cannot work without considering routing table in the authentication layer. Therefore, the scheme cannot be used in the network whose topology of nodes often changes. Also the scheme cannot be used in the situation which cannot use routing tables. Thus, it is necessary to consider a method by separating each layer to use the on demand distributed management even in the situation above.

3 Table Independence Type

Here, we propose an on demand distributed public key management which can separate the routing and authentication layers. In the proposed scheme, each node sends a packet which does not contain routing tables by unicasting. The proposed scheme can be applied to various communication protocols and simple terminals because the scheme does not need to consider routing tables in the authentication layer. Also, the proposed scheme can be used even in the network whose topology of nodes often changes.

3.1 Initial Phase of Authentication

Step 1) Creation of Key Pairs

This step is the same as the conventional system[6].

Step 2) Issuing and Storing of Public key Certificates

In the table independence type, an issuer of the certificate maintains the certificates in own repository. However, the issuer informs the issued fact to Trusted nodes. As a result, each node can omit the operation to send the issued certificates to the Trusted nodes.

Step 3) Certificate Exchange

The exchange process of the repository information is unnecessary.

3.2 Creation of a Certificate Chain

3.2.1 Difference between Table Consideration Type and Table Independence Type

Fig.3 shows how to send the search packet in both protocols. In this figure, the colored nodes are the Trusted nodes. As shown in Fig.3, a node of the table consideration type sends the search packet to neighbor nodes by broadcasting. On the other hand, in the table independence type, each node sends the search packet to Trusted nodes by unicasting, and can send the search packet to all of the Trusted nodes without

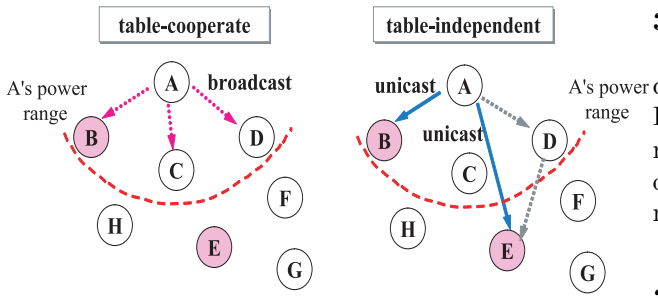

Figure 3: How to send the search packet in both protocols.

considering the routing tables in the authentication layer.

3.2.2 Search Packet

Fig.4 shows a content of a search packet in the table independence type. The following information fields are added to the request packet.

- Authnode: Request node field. This denotes an ID of the node who authenticates other nodes.
- Authednode: Authenticated node field. This denotes an ID of the node who is authenticated finally.
- Source: Source node field. This denotes an ID of the node who sends the search packet.
- Destination: Destination field. This denotes an ID of the node who receives the search packet.

Source and Destination fields are added to make nodes know both a source node and a destination node at that time. Fig.4(1) shows a search packet that the Authenticate node 1 sends. The node 1 makes the Destination of the search packet node 2 and 5 that are Trusted nodes. Then, the node 1 adds its own certificate to each search packet.

3.2.3 Construction of Approach Path

Fig.5 shows an authentication model in the table independence type. As shown in Fig.5(1), the node 1 sends the search packet to its Trusted nodes by unicasting. As a result, the node 2 which is not in the power range of the node 1 can also receive the search packet. In the case that the Trusted node does not trust the Authenticated node, it has to send the search packet to nodes that it trusts. First, the Trusted node adds an own certificate to the search packet. Next, the Trusted node rewrites the Destination field of the search packet to the information of the nodes that it trusts. Then, the Trusted node sends the search packet to its Trusted nodes by unicasting as shown in Fig.5(2).

3.2.4 Construction of Return Path

The Trusted node 3 which sends a reply packet that contains all certificates of the certificate chain to the Request node by unicasting as shown in Fig.5(3). By receiving this reply packet, the node 1 can get all of the certificates $1 \rightarrow 2$, $2 \rightarrow 3$,$3 \rightarrow 4$, which are required for constructing the certificate chain.

3.3 Verification of a Certificate Chain

The Request node 1 needs the following process in order to verify the validity of public keys and certificates that create a certificate chain.

3.3.1 Verification of Public Kyes

To verify the validity of the public keys that form the certificate chain, the Request node uses a digital signature. By the certificate chain $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$, the Request node 1 recognizes that the signatory of the Authenticated node 4's public key is node 3. Then the Request node 1 decrypts the digital signature of the node 3 by using node 3's public key which is contained in the certification of node 3. And the Request node 1 compares the decryption result with the node 3's public key to check whether the decryption is falsified. If they match perfectly, the Request node 1 can verify the justification of node 4's public key. Similarly, the Request node 1 verifies the validity of node 3's public key and node 2's public key that are the rest of the public keys which form the certificate chain.

3.3.2 Verification of Certificates

The certificate turns into effective information when the node authenticates, since our proposed system can collect the certificates of the certificate chain on demand. Consequently, our proposed system doesn't need to confirm the validity of certificates periodically to issuers. As a result, our proposed system does not need a Certificate Revocation List(CRL)[7]-[8].

In our proposed system, the certificates collected for authentication are deleted after completing authentication.

4 Performance Evaluation

4.1 Comparison of Table Consideration Type and Table Independence Type

Table 1 shows a comparison of table consideration type and table independence type. As well as the table consideration type, the table independence type does not need the pre collections of all certificates, since it collects effective certificates on demand. As a result, the table independence type does not have to manage a CRL,too. Compared with the table consideration type that needs to consider the routing

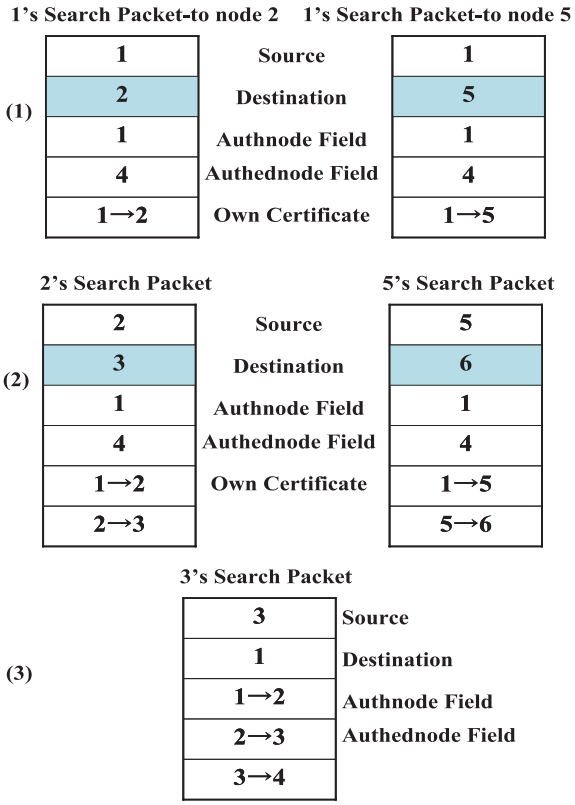

Figure 4: Content of a search packet in the table independence type.

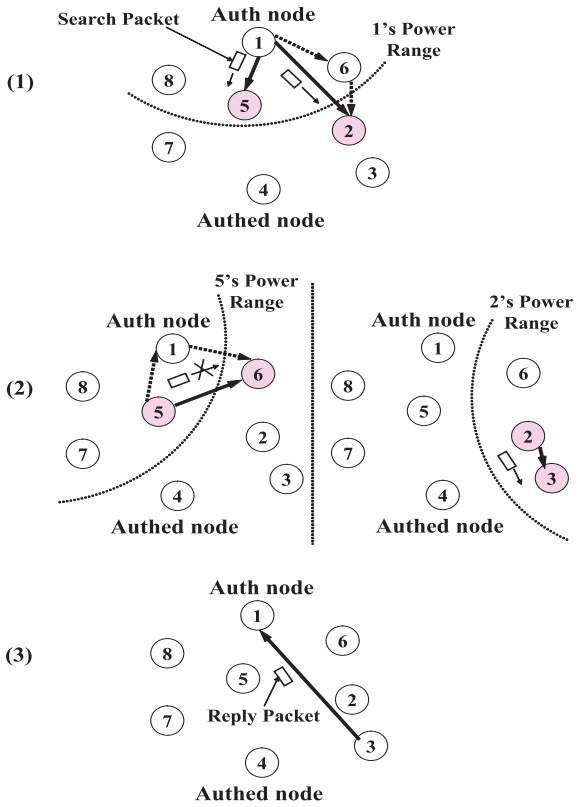

Figure 5: Authentication model in the table independence type.

Table 1: Comparison of Table Consideration Type and Table Independence Type.

Evaluation Item	Consideration	Independence
Pre collections	Unnecessary	Unnecessary
How to collect certificates	On demand	On demand
Update CRL	Unnecessary	Unnecessary
Consideration of Routing tables	Necessary	Unnecessary

protocols in the authentication layer, the table independence type does not have to consider the routing tables, since nodes collect certificates by unicasting in the routing layer.

4.2 Simulation Scenario

- There is at least one certificate that the node issued and that other nodes issued to her.
- A Request node and an Authenticated node are chosen in the same procedure.
- The number of average trusted nodes per node assumes to be uniformly distributed.

4.3 Completing Probability of a Certificate Chain

Fig. 6 shows a completing probability of a certificate chain versus the number of average trusted

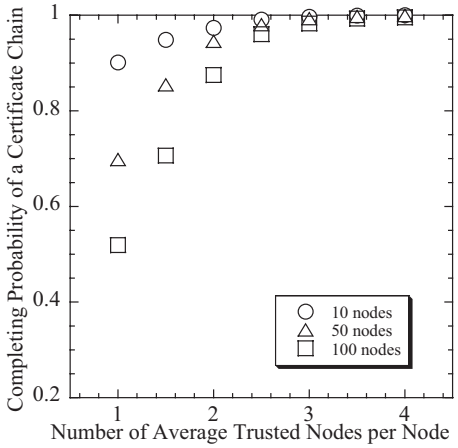

Figure 6: Completing probability of a certificate chain.

nodes per node. As shown in Fig. 6, the proposed system can certainly construct the certificate chain by trusting four nodes at least in average.

4.4 Average Traffic

Fig.7 shows average traffic when the node collects effective certificates versus simulation region which is a length(m) of a quadrangle. Here, we call

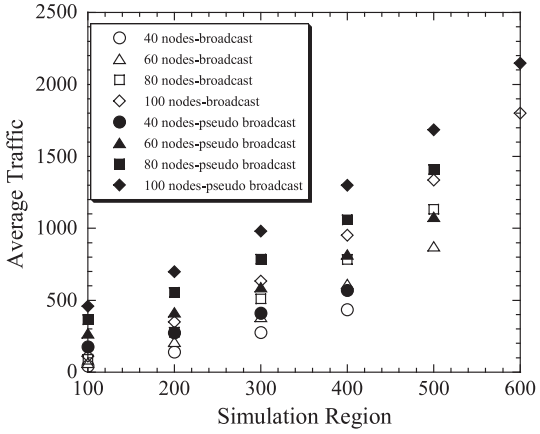

Figure 7: Average traffic.

the way to find the certificates of the certificate chain in the table independence type 'pseudo broadcast'. As shown in Fig.7, the average traffic of the table independence type is larger than the table consideration type. However, the table independence type does not need to consider routing tables in the authentication layer. Therefore, the both scheme can be used properly by the usage. The table independence type can be used in the network which topology of nodes often changes.

5 Conclusion

We have proposed an on demand distributed public key management which can separate the routing and authentication layers. In the proposed scheme, each node sends a packet which does not contain routing tables by unicasting. The proposed scheme can be applied to various communication protocols and simple terminals since the scheme does not need to consider routing tables in the authentication layer. Also, the proposed scheme can be used even in the network whose topology of nodes often changes. By a computer simulation, we find that the scheme can be used in the network which topology of nodes often changes.

6 Acknowledgment

This work is partly supported by Keio University 21st century COE program on "Optical and Electronic Device for Access Network".

References

[1] http://www.ietf.org/html.charters/prix-charter.html.

[2] S. Corson and J. Macker, "Mobile ad hoc networking(MANET):
Routing protocl performance issues and evaluation consideration," IETF RFC25010,Jan,1999.

[3] Mobile Ad-hoc Networks(manet)Charter, http://www.ietf.org/html.charters/manet-charter.html.

[4] C.E. Perkins, *Ad Hoc Networking*. Addison Wesley Professional, Dec. 2000.

[5] J. Jubin and J.D. Turnow, "The DARPA Packet Radio Project," *Proc.IEEE*, 1987.

[6] "On Demand Distributed Public Key Management using routing information for Wireless Ad Hoc Networks," Computer Security Symposium, Oct 2004.

[7] "ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection- The Directory: Public-Key and Attribute Certificate Frameworks," ITU-T, March 2000.

[8] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC-2459, January 1999.

[9] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," Comput.Commun.Rev, pp.234-244,1994.

[10] S. Murthy and J.J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," ACM MONET Journal, pp.183-197,1996.

[11] C.-C. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "Routing in clustered mutihop, mobile wireless networks with fading channel," Proceedings of IEEE SIngapore International Conference on Networks(SICON'97),1997.

[12] P. Jacquet, P. Muhlethaler, A. Qayyum, A. Laouiti, L. Viennot, and T. Clausen, "Optimized link state routing protocol," Internet-draft, draft-ietf-manet-olsr-02.txt,2000.