Development of certificate based secure communication for Mobility and Connectivity protocol

Yuya Miyazaki*, Katsuhiro Naito†, Hidekazu Suzuki‡, Akira Watanabe‡,
*Graduate School of Business Administration and Computer Science, Aichi Institute of Technology,
Nagoya, Aichi 464-0807, Japan, Email: miyazaki121@pluslab.org
†Faculty of Information Science, Aichi Institute of Technology, Toyota, Aichi 470-0392, Japan, Email:naito@pluslab.org
‡Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 468-8502, Japan

***Abstract*—Some Internet of Things (IoT) devices for smart lock systems, home management systems have been released in recent years. Almost all services employ a client-server model because direct communication among these devices is difficult due to the Network Address Port Translation (NAPT) mechanism. Recently, some new ideas such as a fog computing and an edge computing have been proposed to create a distributed service. A direct communication is suitable for these ideas because each service devices should communicate with each other to realize a distributed processing. The authors have been developed Network Traversal with Mobility (NTMobile) which is a protocol for realizing a direct communication between devices and a secure communication. This paper extends the secure communication mechanism of NTMobile to realize a direct encryption key exchange mechanism between devices by employing the technology of Public Key Infrastructure (PKI). The developed protocol can provide a mutual authentication mechanism and secure encryption key exchange mechanism among devices. The evaluation results show that the overhead of the developed implementation is not large in practical services comparing to the conventional key exchange mechanism of NTMobile.**

I. Introduction

Internet of Things (IoT) devices has been increasing rapidly in recent years. Internet Protocol (IP)v4 is a main network protocol in the current Internet infrastructure technology. Since the stock of IPv4 global addresses is running low, Network Address Port Translation (NAPT) mechanism has been introduced in practical networks. Therefore, end-to-end communication is becoming impossible because a NAPT router blocks communication from the Internet side[1], [2]. Additionally, IPv6 is also introduced into new networks because the number of IPv6 addresses is almost infinity. Therefore, incompatibility between IPv4 and IPv6 is a new issue in a recent Internet. The client server model is a simple way to solve the above issues: the blocking due to NAPT routers and the incompatibility between IPv4 and IPv6. On the contrary, a redundant path through a server may be overhead for throughput and communication delay, and relaying data at the server may be a risk of eavesdropping communication between devices. Direct communication between devices is also a simple solution for these issues in IoT services. Some researchers have proposed new mechanisms to ensure communication connectivity[3], [4], [5] because direct communication between devices has various advantages such as network traffic mitigation and improvement in communication speed, communication delay etc.

Many devices implement a plurality of wireless communication technologies to connect to the Internet. Therefore, choosing a network interface with a good communication status can improve communication quality. On the contrary, all communication sessions are reset due to change of an IP address because different access networks have their own network address. Previous studies have proposed a network mobility technique to separate the location information and an identifier. Applications can realize continuous communication by separating these information when the IP address changes due to switching networks[6], [7], [8], [9].

The authors have been developing a feasible implementation that is called Network Traversal with Mobility (NTMobile) to solve these issues [10], [11]. NTMobile system consists of Account Server (AS), Direction Coordinator (DC), Relay Server (RS), and end-devices. AS provides authentication function of each end-device, and establishes a relationship of trust among the system. DC provides virtual IP addresses to each end-devices to realize continuous communication. It also directs each end-device to realize end-to-end communication according to registered network information of them. Conventional NTMobile provides an encryption key sharing mechanism between end-devices. On the contrary, some encryption keys are carried through the servers.

This paper introduces a Public Key Infrastructure (PKI) to NTMobile to enhance the encryption key sharing mechanism to avoid key exchange through the servers. The developed protocol can provide a mutual authentication mechanism and secure encryption key exchange mechanism among devices. The evaluation results show that the overhead of the developed implementation is not large in practical services comparing to the conventional key exchange mechanism of NTMobile.

II. NTMobile

Fig. 1 shows the overview of NTMobile system. NTMobile system consists of Account Server (AS), Direction Coordinator (DC), Relay Server (RS), and NTMobile nodes. DC assigns Fully Qualified Domain Name (FQDN) and a virtual IP address to a NTMobile node to identify each NTMobile node and to realize the IP mobility. NTMobile recognizes the name resolution procedure for a correspondent NTMobile node as a trigger for the NTMobile procedure. An initiation NTMobile node can obtain a real IP address and a virtual IP address of a correspondent NTMobile node. The virtual IP address is notified to an application as a result of the

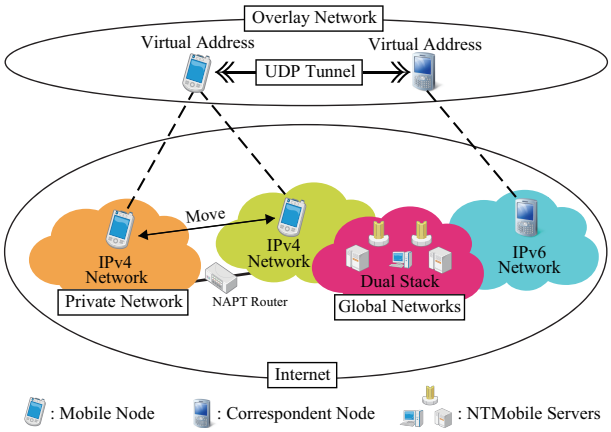

Fig. 1. System model of NTMobile.

name resolution. Therefore, the application can start a session to the correspondent NTMobile node. Since the virtual IP addresses are stable during the session, NTMobile nodes can communicate with each other continuously even if the nodes switch an access network. As a real communication, IP datagrams including the virtual IP addresses are capsulated by real IP addresses. The encapsulated IP datagrams are carried over a User Datagram Protocol (UDP) tunnel. The application on the correspondent NTMobile node can receive decapsulated IP datagram including the virtual IP addresses. The following shows the details of the components.

- Direction Coordinator (DC)
  The function of DC is to manage location information of each NTMobile node. Communication connectivity can be performed according to the registered network information of each NTMobile node. Additionally, each DC has the DNS function to realize distributed management of network information, and registers its FQDN as Name Server (NS) record. Therefore, each DC can easily find another DC by querying NS records.
- Account Server (AS)
  The function of AS is to authenticate NTMobile nodes. It also distributes a shared encryption key to DC when it accepts the authentication request from NTMobile nodes. NTMobile nodes can communicate with DC by using the distributed shared encryption key.
- Relay Server (RS)
  RS relays a tunnel between NTMobile nodes when they cannot communicate directly due to a NAT traversal and difference of the IP protocol version. Since a communication encryption key is exchanged between NTMobile node with a temporal encryption key, RS cannot decrypt the tunnel communication.
- NTMobile node
  NTMobile node accesses AS to request an authentication and to obtain a shared encryption key between DC and a NTMobile node. Then, it accesses to its assigned DC to register its own network information. It also requests a tunnel establishment to the DC when it starts to communicate with a correspondent node. Since the DC directs a procedure for the tunnel establishment between NTMobile nodes, they can set up the communication tunnel.

A. Conventional key exchange scheme

Since each server such AS, DC, and RS has own common key to communicate with each other by using Secure Sockets Layer / Transport Layer Security (SSL/TLS) , every communication among the servers is securely encrypted. NTMobile nodes and their DC also have a shared encryption key. NTMobile system uses the following three encryption key to realize secure communication between NTMobile nodes.

- End key
  The end key is used for encryption of tunnel communication. MN generates the end key.
- Temporary key
  The temporary key is used for the end key encryption. The DC delivers the temporary key to the NTMobile nodes by the route direction message. Therefore, RS does not receive the temporary key, and does not decrypt the end key in the tunnel request message.
- Tunnel key
  The tunnel key is used for the tunnel request message encryption. DC distributes the tunnel key to the NTMobile nodes by transmitting the route direction message. RS also receives the tunnel key by the relay direction message.

In the conventional method, the end key can be revealed when the tunnel key and the temporary key is leaked by server hacking.

III. Proposed Key Exchange Scheme

The proposed key exchange scheme introduces PKI to the NTMobile system to enhance the secure communication. It also extends the certificate chain in the NTMobile network to issue a certificate to each NTMobile node. An initiation NTMobile node encrypts an end key by a public key with its certificate. As a result, the end key can be shared between NTMobile nodes securely. Additionally, each NTMobile node can authenticate each other by using their certificates.

A. Introducing PKI

In the conventional NTMobile scheme, an end key is encrypted by a temporary key, which is distributed from DC. The NTMobile nodes in the proposed scheme encrypt the end key with the certificate instead of the temporary key.

Fig 2 shows the extended certificate chain. The proposed scheme adds the intermediate certificate authority into AS as a new additional function. Therefore, AS issues a certificate to the NTMobile nodes. Further, it is necessary to introduce a Certificate Revocation List (CRL) to manage issued certificates. Details of the extended NTMobile functions are as following.

- Extension of AS functions
  We extend AS functions to support certificate issuance and revocation. AS verifies the certificate to validate NTMobile nodes in the authentication process. It also

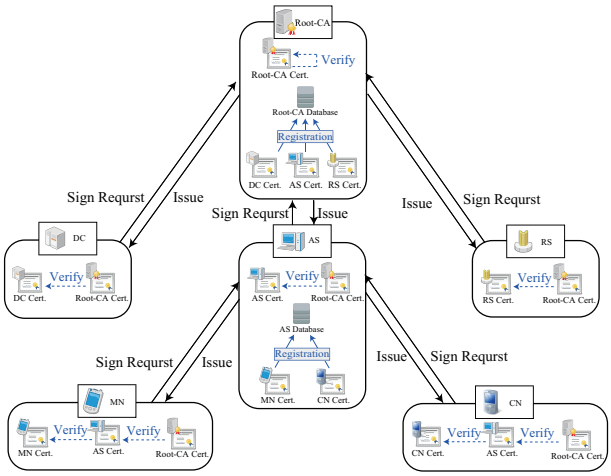

Fig. 2. Extended certificate chain

notifies the latest information on NTMobile nodes when it issues a new certificate and revokes certificates. The notification includes serial numbers and validity of issued and revoked certificates.

- Extension of DC functions
  DC sends the serial number and the status of the certificate by transmitting a route direction message when the NTMobile nodes requests a tunnel establishment. This function imitates Online Certificate Status Protocol Responder. Therefore, we extend the database of DC to manage these information. Additionally, DC also supports the notification from AS to inform an issuance and a revocation.
- Extension of NTMobile node functions
  NTMobile nodes should manage their certificate in the proposed scheme. Since the certificate chain of NTMobile system has own root certificate, NTMobile nodes should store the root certificate and an intermediate certificate authority of AS.

B. Extension of the signaling

In the following explanation, we define the initiator NTMobile node as Mobile Node (MN), and responder NTMobile node as Correspondent Node (CN). Details of the proposed signaling are as following.

Fig 3 shows the signaling of the tunnel establishment process. The signaling process starts when MN transmits the direction request message to DC_{MN}. MN attaches its certificate to the direction request message to validate each other. DC_{MN} obtains information about CN by exchanging the node information request / response messages to DC_{CN} . The obtained information includes the network information, the virtual IP address, the serial number and the status of certificate for CN. DC_{MN} determines an appropriate tunnel route according to the network information of MN and CN. Then, the determined route is notifies to MN and CN in the route direction message. The route direction message includes a certificate serial number and the certificate for both NTMobile nodes. Finally, each NTMobile node can obtain the

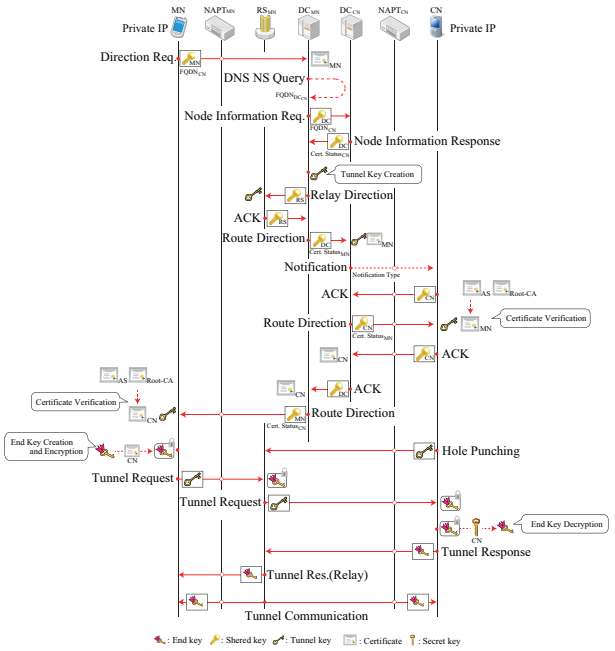

Fig. 3. Tunnel establishment process

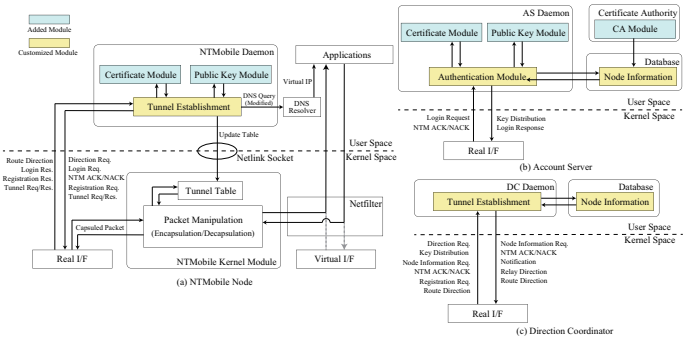

Fig. 4. Implemented modules

certificate of the other node.

Since the certificate is obtained by the route direction message, the certificates are used to validate each other at the beginning of the process. Verification examines four points: the digital signature, the serial number, FQDN, and the expiration date. Both NTMobile nodes can validate each other because the serial number is attached in the route direction message, and the extra information is included in the certificate. After the validation of the certificate, MN generates an end key for encryption and encrypts it with the public key of the certificate of CN. Then, it sends the encrypted end key in the tunnel request message to CN. Finally, MN and CN can share the end key by decrypting it with the secret key of CN.

IV. Implementation

Fig 4 shows the implemented module model. The public key module and the certificate module are added at NTMobile nodes and AS. The certificate module performs the verification and the conversion of the certificate format. The public key module is used for the public key algorithm to encrypt and

TABLE I
SPECIFICATION

Host Machine	
OS	OS X 10.9.5
CPU , Memory	Intel Core-i7 2.8GHz , 16 GBytes
Software	VirtualBox 5.0
Virtual Machine	
OS	Ubuntu 12.04
Memory	512 MBytes
Certificate	X509v3 SHA256 with RSA
Public key cryptosystem	RSA 2048bit
Common key cryptosystem	AES-CFB 128bit
Number of measurements	10

TABLE II
TUNNEL ESTABLISHMENT TIME

	Time[ms]	
	Conventional model	Proposed model
DC 1 unit	37.8	92.2
DC 2 unit	65.1	138.7

decrypt data. AS has a Certificate Authority (CA) module to provide a function of the intermediate certificate authority to issue a certificate to NTMobile nodes. The authentication module and tunnel establishment module are extended due to a change in the message format.

V. EVALUATION

Fig. 5 shows the virtual machine network for the experimental evaluation. Tab. I shows the specification of the evaluation environment. In the evaluation, we discuss the overhead of the tunnel establishment process of the proposed model. The measurement results are an average of 10 times for evaluations.

Tab. II shows the processing period of the tunnel establishment procedure. Fig. 6 shows the measurement results at the time of message processing at two DCs. The overhead period of the proposed model with one DC was about 54.4 ms and that with two DCs was about 73.6 ms. Additionally, about 80% of the total overhead are message processing for direction request messages, NTM ACK messages, and route direction messages because these messages include a certificate. The main reason of the overhead is the calculation of an encryption or a Message Authentication Code (MAC). The second largest overhead is the tunnel establishment process. The results show that the overhead is about 16 ms. The overhead comes from the public key cryptosystem. We have confirmed that the overhead of the proposed model is not a big issue because typical wireless communication link has similar delay period.

VI. CONCLUSION

This paper has proposed a new security mechanism based on PKI for NTMobile. The proposed mechanism can employ a certificate to enhance secure communication between NTMobile nodes. As a result, NTMobile nodes can authenticate each other and can exchange an encryption key securely. The developed implementation performs the enhanced secure communication without large overhead comparing to the conventional NTMobile security mechanism that employs common keys.

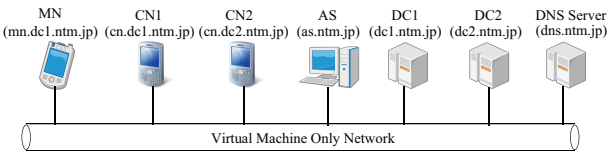

Fig. 5. Evaluation Model

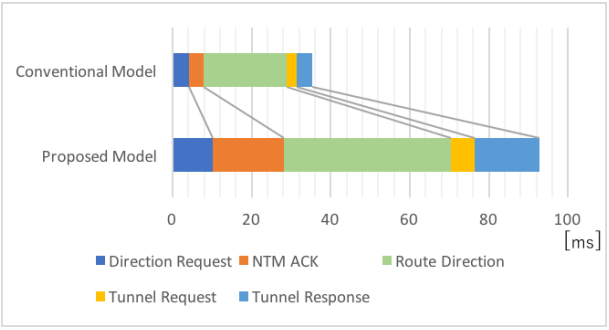

Fig. 6. Message Overhead

ACKNOWLEDGMENT

This work is supported in part by Grant-in-Aid for Scientific Research (B)(15H02697) and (C)(17K00142), Japan Society for the Promotion of Science (JSPS), and the Hibi science foundation.

REFERENCES

[1] H. Levkowetz and S. Vaarala, "Mobile ip traversal of network address translation (nat) devices," Tech. Rep., 2003.

[2] I. Society. Ip addressing issues. [Online]. Available: http://www.internetsociety.org/ip-addressing/

[3] S. Niazi and J. Dowling, "Usurp: Distributed nat traversal for overlay networks," *Proceedings of the 11th IFIP WG 6.1 International Conference on Distributed Applications and Interoperable Systems*, June 2011.

[4] D. W. J. Rosenberg, R. Mahy, "Session traversal utilities for nat (stun) session traversal utilities for nat (stun) session traversal utilities for nat (stun) session traversal utilities for nat (stun)," *RFC 5389*, October 2008.

[5] J. Rosenberg, "Interactive connectivity establishment (ice): A protocol for network address translator (nat) traversal for offer/answer protocols," *RFC 5245*, April 2010.

[6] M. ISHIYAMA, M. KUNISHI, K. UEHARA, H. ESAKI, and F. TERAOKA, "Lina: A new approach to mobility support in wide area networks (special issue on internet technology)," *IEICE transactions on communications*, pp. 2076–2086, August 2001.

[7] X. F. D. Le and D. Hogrere, "A review of mobility support paradigms for the internet," *IEEE Communica- tions surveys*, pp. 38–51, March 2006.

[8] H. Soliman, "Mobile ipv6 support for dual stack hosts and routers," *RFC 5555*, June 2009.

[9] J. A. C. Perkins, D. Johnson, "Mobility support in ipv6," *RFC 6275*, July 2011.

[10] K. Naito, T. Nishio, K. Mori, H. Kobayashi, K. Kamienoo, H. Suzuki, and A. Watanabe, "Proposal of seamless ip mobility schemes: Network traversal with mobility (ntmobile)," *Global Communications Conference (GLOBECOM)*, pp. 2572–2577, December 2012.

[11] K. Naito, K. Mori, H. Kobayashi, K. Kamienoo, H. Suzuki, and A. Watanabe, "End-to-end ip mobility platform in application layer for ios and android os," *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 92–97, January 2014.