Evaluation of a Secure End-to-End Remote Control System for Smart Home Appliances

Hisayoshi Tanaka, Hidekazu Suzuki and Akira Watanabe
Graduate School of Science and Technology
Meijo University
Aichi, Japan 468–8502

Katsuhiro Naito
Faculty of Information Science
Aichi Institute of Technology
Aichi, Japan 470–0392

***Abstract*—In most existing remote-control services for smart home appliances, a controller outside the home network can be used to control these appliances in the home network using a remote-control support server installed on the Internet. However, if the service provider ends the service, a user cannot control these appliances from outside the home. To solve this problem, we have proposed a secure end-to-end remote-control system based on the "Network Traversal with Mobility," which can solve a NAT traversal problem and achieve end-to-end encrypted communication and IP mobility. In this study, we implemented a prototype of the proposed system and conducted a remote control experiment and performance evaluation for smart home appliances compliant with ECHONET Lite. Consequently, a user could directly access ECHONET Lite appliances inside the home from outside the home network with a low delay without any remote-control support server.**

I. Introduction

With the progress of the Internet of things (IoT) technology, smart home products for a connected home, such as security cameras, smart door locks, and smart appliances, are attracting attention. In Japan, smart home appliances compliant with ECHONET Lite, which is the home energy management system standard, are on the market. In addition, remote-control services for these products have become increasingly popular in ordinary homes [1]. A user outside its own home can remotely control ECHONET Lite devices inside the home using these services. To achieve these services, a remote-control support (RCS) server is installed on the internet by a smart-appliance manufacturer, and has a function of transferring ECHONET Lite messages from the user to the appliances in the home network. However, if the services are ended, a user cannot control these appliances from outside the home. In addition, there is a concern that the operation log stored in the server could be leaked and that the privacy of the users might be infringed.

To solve these problems, authors have proposed a secure end-to-end remote-control system [2]. The proposed system is based on the "Network Traversal with Mobility" (NTMobile) [3], which can solve a network address translator (NAT) traversal problem and achieve end-to-end encryption communication supporting the migration of the IP layer. In the proposed system, the remote-control service for the ECHONET Lite devices could be achieved without any RCS server.

In this study, we implement a prototype of the proposed system and conduct a remote control experiment for the ECHONET Lite devices. Furthermore, we evaluate the response time required for the remote control of these devices, and show the usefulness of the proposed system.

II. Outline of The Proposed System

The proposed system consists of the following four types of devices. A mobile node (MN) is an ECHONET Lite controller wherein the extended NTMobile is installed, which exists in a foreign network. An ECHONET Lite device (ELD) is a commercially available home appliance, which exists in a home network. A remote control agent (RCA) is a home device newly defined using the proposed system and has functions of the extended NTMobile including a virtual IP address allocation for ELDs and an address translation similar to a NAT router. A direction coordinator (DC) is a server installed on the Internet for establishing an encrypted user datagram protocol (UDP) tunnel between NTMobile-ready devices. When MN and RCA communicate through this UDP tunnel, all IP packets addressed to each other's virtual IP address are encrypted.

Fig. 1 shows the communication sequence in the proposed system. When an ECHONET Lite application in the MN multicasts a device search message, the extended NTMobile function starts a tunnel establishment procedure with the RCA

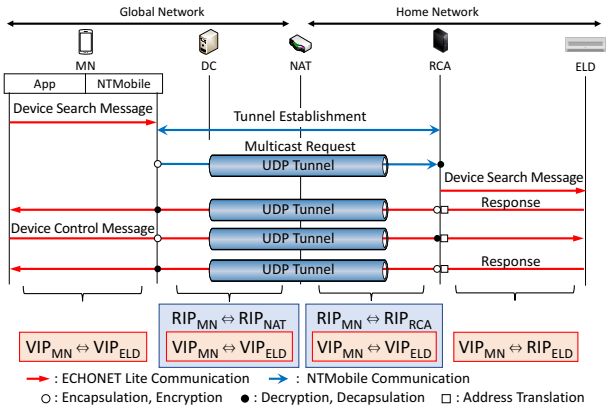


Fig. 1. Communication sequesnce in the proposed system

with the support of the DC. After establishing an encrypted UDP tunnel, the MN sends a multicast request message to the RCA to request a search for ELDs. The RCA searches ELDs in the home network and receives the response message from the ELDs. Here, the RCA internally allocates an unused virtual IP address to the discovered ELD and records the association between the virtual and real IP addresses in the address allocation table (AAT). Thereafter, the RCA translates the real IP address of the ELD described in the response message ($\mathrm{RIP_{ELD}}$) to the associated virtual IP address ($\mathrm{VIP_{ELD}}$), and then transfers it to the MN through the UDP tunnel. Using the above procedure, the ECHONET Lite application discovers the ELDs in the home network and recognizes the IP address of each appliance with the virtual IP address.

When remotely controlling the discovered appliance, the MN sends an ECHONET Lite control message to $\mathrm{VIP_{ELD}}$ by reusing the encrypted UDP tunnel. The RCA decrypts and decapsulates the packet, and subsequently translates its destination address from $\mathrm{VIP_{ELD}}$ to $\mathrm{RIP_{ELD}}$ based on the AAT. The control message is transferred to the ELD, which the MN wishes to control. The ELD processes the message and the response is sent to the MN using the reverse procedure. With this procedure, these messages are mutually transferred between MN and ELD without an RCS server.

III. Implementation and Evaluation

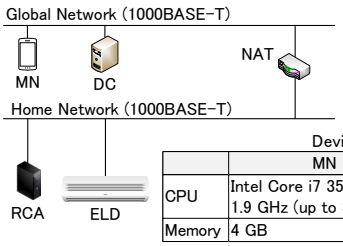
A. Implementation

We implemented a prototype of the proposed system using Linux PCs. The MN installed an NTMobile kernel module and an NTMobile daemon. The kernel module hooks the multicast packets with a netfilter and sends them to an NTMobile daemon via the netlink socket. The daemon starts the NTMobile signaling procedure. The RCA also installed the kernel module and the daemon. In addition, the address translation function in the RCA was achieved using the iptables. The kernel module has a packet manipulation function such as encapsulation/decapsulation and encryption processing using the AES implemented in the Linux kernel.

B. Evaluation

We conducted a remote control experiment with the prototype system and evaluated the communication delay. Fig. 2 shows the experimental environment. The DC is run as a Linux virtual machine on a VMware vSphere Hypervisor 4.1 (ESXi 4.1). The MN and the DC were installed on the global IPv4 network built in our laboratory. The ELD was a commercial room air conditioner (TOSHIBA RAS-B806DRH) and was installed on our laboratory network behind the NAT router. We used Wireshark to measure the response times between MN and ELD. For further information, the round-trip time (RTT) between each device is as shown in Fig. 2.

TABLE I shows the average values of the measurement results. It was confirmed that the tunnel establishment processing based on the NTMobile, device discovery processing, and device control processing were completed in an extremely short time. However, it should be noted that these results do not include the internet delay. Assuming that the RTT between devices in the actual Internet environment is approximately 100 ms, the response times in the proposed system will be approximately 450 ms for device discovery involving the tunnel establishment processing[1] and approximately 170 ms for device control. In the ECHONET Lite specification, the timeout period from the transmission of a control message to the reception of a response message is defined as 5,000 ms. Therefore, we found that the overhead in the proposed system did not adversely affect the ECHONET Lite communication. We also proved that the proposed system could achieve a secure remote control service without using the RCS server provided by the manufacturer.



Average of RTT

	Time (ms)
MN – DC	0.47
DC – RCA	1.27
MN – RCA	0.93
RCA – ELD	0.67

Device Specifications

	MN	RCA
CPU	Intel Core i7 3517U 1.9 GHz (up to 3.0 GHz)	Intel Celeron N2830 2.16 GHz (up to 2.41 GHz)
Memory	4 GB	8 GB

Fig. 2. Experimental envirionment

TABLE I
Response time

	Time (ms)
Tunnel establishment	48.90
Device discovery	10.03
Device control	73.00

IV. Conclusion

In this paper, we evaluated a secure end-to-end remote control system for ECHONET Lite appliances and confirmed that it could be achieved. This system can be applied not only to ECHONET Lite but also to other services that remotely control smart home products via servers. Since control messages do not pass through the server on the Internet, there is no concern that the operation history will remain in the server, and a safe and trusted remote control service can be provided to users.

Acknowledgement

This research was supported by a research grant of the Naito Science & Engineering Foundation.

References

[1] H. Sumino, Y. Uchida, N. Ishikawa, H. Tsutsui, H. Ochi, and Y. Nakamura, "Home Appliance Control from Mobile Phones," in *Proc. of IEEE CCNC 2007*, May 2007, pp. 793–797.

[2] H. Tanaka, H. Suzuki, K. Naito, and A. Watanabe, "Proposal for a Secure Remote Control System for ECHONET Lite Home Appliances," in *Proc. of IEEE GCCE 2017*, Oct. 2017, pp. 310–311.

[3] H. Suzuki, K. Naito, K. Kamienoo, T. Hirose, and A. Watanabe, "NTMobile: New End-to-End Communication Architecture in IPv4 and IPv6 Networks," in *Proc. of ACM MobiCom 2013*, Oct. 2013, pp. 171–174.

[1] NTMobile signaling messages are exchanged one round trip between MN and DC, between DC and RCA and between MN and RCA, respectively.