A Proposal for Secure Remote Control System for ECHONET Lite 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*—On most existing remote-control services for ECHONET Lite devices, a controller outside the home network can control ECHONET Lite devices in the home network by using a remote-control support server on the Internet. However, if the service provider ends the service, a user cannot control these devices from the outside of the house. This paper proposes a secure remote-control system based on Network Traversal with Mobility (NTMobile), which can solve a NAT traversal problem, achieve end-to-end encryption communication and IP mobility. With the proposed system, the controller can directly access in-house ECHONET Lite devices from the outside of the home network without any remote-control support server. In addition, since the operation log is not stored in the service provider, it is possible to achieve a safe and trusted remote-control system with due consideration to privacy of users.**

I. Introduction

With the spread of mobile devices such as smartphones and tablet computers, remote-control services for home appliances become popular in ordinary homes [1]. A user outside the home can remotely control home appliances compatible with ECHONET Lite in the home by utilizing these services. ECHONET Lite is the most widely recognized standard protocol for controlling and managing these appliances in Japan. In order to achieve these services, home appliance manufacturers install a remote-control support server on the Internet. The server has a function to transfer ECHONET Lite control messages from the user to appliances in the home network. However, if the manufacturer ends the service, a user cannot control these appliances from the outside of the house. In addition, there is also concern that the operation log stored in the server is leaked and user's privacy may be infringed.

In order to solve these problems, this paper proposes a secure remote-control system based on Network Traversal with Mobility (NTMobile) [2]. NTMobile can solve a NAT traversal problem and achieve end-to-end encryption communication. In the proposed system, the remote-control service for ECHONET Lite-compliant appliances could be achieved without any remote-control support server.

II. NTMobile System

NTMobile is an End-to-End communication architecture that can achieve connectivity and mobility simultaneously in IPv4/IPv6 networks. In the NTMobile architecture, NTMobile-compatible nodes (NTM nodes) establish a connection by their virtual IP addresses which are not existed in real networks. All packets based on virtual IP addresses are encrypted and sent through a UDP tunnel between NTM nodes. Consequently, applications running in each NTM node can make communication without being affected by existence of NAT on the communication path.

A Direction Coordinator (DC) is a server to manage address information of NTM nodes and directs NTM nodes to establish UDP tunnels. The address information includes FQDN, real IPv4 and IPv6 addresses, virtual IPv4 and IPv6 addresses, and IPv4 global IPv4 address of NAT router when the NTM node is behind the NAT router.

III. Our Proposed System

A. System Configuration

Fig. 1 shows the system configuration of the proposed system and the state of remote control communication. A mobile node (MN) is an ECHONET Lite controller in which the extended NTMobile is installed and exists in the foreign network. An ECHONET Lite device (ELD) is a commercially available home appliance and exists in a home network. A remote control agent (RCA) is a home device newly defined by the proposed system and has functions of the extended NTMobile that are a virtual IP address allocation for ELDs, a management of Address Allocation Table (AAT) and an address translation like NAT router. The MN establishes a UDP tunnel to the RCA according to a direction from the DC on the Internet and sends ECHONET Lite messages to

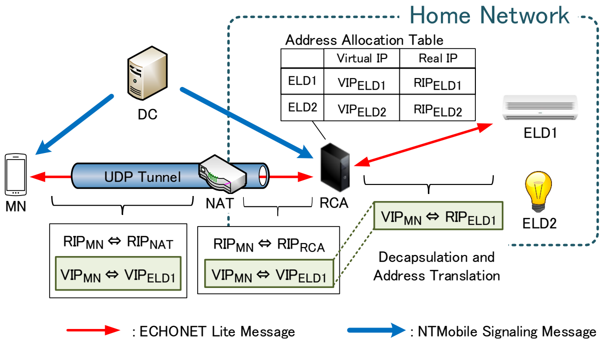
Home Network
Address Allocation Table
Virtual IP
Real IP
ELD1
ELD2
VIP_{ELD1}
RIP_{ELD1}
VIP_{ELD2}
RIP_{ELD2}
DC
MN
UDP Tunnel
NAT
RCA
ELD1
ELD2
$RIP_{MN} \Leftrightarrow RIP_{NAT}$
$VIP_{MN} \Leftrightarrow VIP_{ELD1}$
$RIP_{MN} \Leftrightarrow RIP_{RCA}$
$VIP_{MN} \Leftrightarrow VIP_{ELD1}$
$VIP_{MN} \Leftrightarrow RIP_{ELD1}$
Decapsulation and
Address Translation
: ECHONET Lite Message
: NTMobile Signaling Message

Fig. 1. Overview of proposed method.

the virtual IP address of ELD (VIP_{ELD}) through the UDP tunnel. The RCA decrypts and decapsulates received messages and then translates the destination address from the virtual IP address to the real IP address of the ELD (RIP_{ELD}) according to the AAT. With this procedure, these messages are mutually transferred between MN and ELD without a remote-control support server.

B. Communication Sequence

In the existing NTMobile architecture, a UDP tunnel establishment procedure is started with the detection of the DNS inquiry packet as a trigger. In the proposed system, NTMobile is extended so that tunnel establishment starts with an ECHONET Lite device search message as a trigger.

Fig. 2 shows the device search 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 to the RCA with the support of DC and then sends a Multicast Request to the RCA. The Multicast Request is a newly defined NTMobile signaling message and contains information of the device search message. The RCA generates the device search message according to the received Multicast Request and multicasts it to the home network.

After receiving the multicasted message, ELDs send a reply message back to the MN's virtual IP address (VIP_{MN}). In the proposed system, packets addressed to the virtual IP address are received on behalf of the RCA. The RCA internally allocates an unused virtual IP address to the ELD that sent the reply message and records the virtual and real IP addresses in the AAT in association with each other. After that the RCA translates the source address of the reply message from RIP_{ELD} to VIP_{ELD} and then transfers it to MN through the UDP tunnel. Through the above procedure, the ECHONET Lite application discovers ECHONET Lite appliances in the home network and recognized the IP address of each appliances with the virtual IP address.

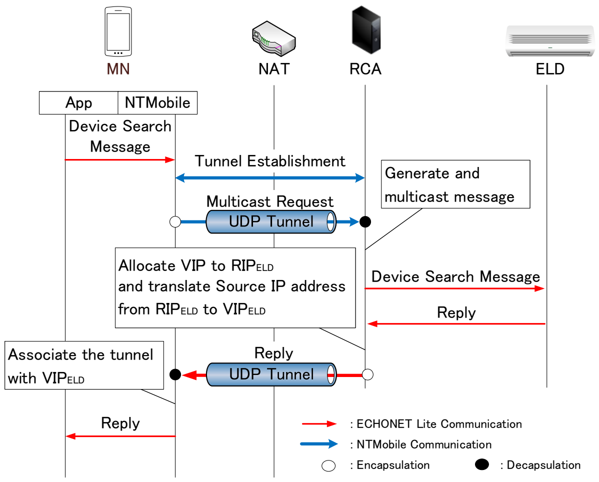

Fig. 2. ECHONET Lite devices search sequesnce

When remotely controlling the discovered appliance, the MN sends an ECHONET Lite control message to VIP_{ELD} by reusing the UDP tunnel established at the device search procedure. The RCA decrypts and decapsulates the packet and then translates its destination address from VIP_{ELD} to RIP_{ELD} according to the AAT. The control message is transferred to the ECHONET Lite appliance that the MN wishes to control. The appliance processes the message and the reply is transferred to the MN by the reverse procedure.

IV. Implementation and Verification

A. Implementation

We extended conventional NTMobile modules to achieve the proposed system. An NTMobile kernel module in the MN has been extended to hook multicast packets with netfilter in addition to DNS packets as before. An NTMobile daemon in the user space of the MN receives the hooked multicast packet via Netlink socket and starts the NTMobile signaling. The AAT and the address translation function in the RCA has been achieved using Linux iptables.

B. Verification

As MN and RCA, we used Linux PC which the extended NTMobile modules are implemented. DC run as a virtual machine on VMware ESXi. MN and DC was installed in the global IPv4 network. ECHONET Lite-compliant appliances installed in the home network were commercial air conditioner and lighting.

With the above configuration, we confirmed that it is possible to remotely control these appliances with ECHONET Lite controller application installed in the MN. As a result of the operation verification, it was confirmed that the MN can search and control these ECHONET Lite appliances without using the remote-control support server provided by the manufacturer.

V. Conclusion

In this paper, we have proposed a secure remote-control system for ECHONET Lite appliances using the extended NTMobile. With the proposed system, a mobile device could control ECHONET Lite appliances in the home network from the outside the home without using the remote-control support server. ECHONET Lite control messages exchanged over the Internet are all encrypted and the operation history is not accumulated in the server. Therefore, a safe and trusted remote control service that can protect the privacy of users could be achieved.

Acknowledgement

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

References

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

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