Proposal for Private Address-Type WoT Server using NTMobile Technology

Kaito Kuromiya
Graduate School of Science and Technology
Meijo University
Aichi 468-8502, Japan
kaito.kuromiya@wata-lab.meijo-u.ac.jp

Hidekazu Suzuki
Graduate School of Science and Technology
Meijo University
Aichi 468-8502, Japan
hsuzuki@meijo-u.ac.jp

Katsuhiro Naito
Information Science
Aichi Institute of Technology
Aichi 470-0392, Japan
naito@pluslab.org

Akira Watanabe
Graduate School of Science and Technology
Meijo University
Aichi 468-8502, Japan
wtnbakr@meijo-u.ac.jp

***Abstract*—NTMobile (Network Traversal with Mobility) is our original technology capable of providing the NAT traversal and secure end-to-end communication. In this paper, we propose a system to set the WoT (Web of Things) server in a private network, and the server is accessed from different private networks by using NTMobile. According to this method, it is possible to construct a secure system preventing server attacks such as DDoS attacks, and also almost all Web programming technologies can be used as they are. We have built the web server in RaspberryPi and set in the private network, and confirmed image communication and remote controls via the Internet.**

***Index Terms*—WoT, NAT Traversal, End-to-End Communication**

I. Introduction

While IoT (Internet of Things) is spreading in the world, there appears so many frameworks, and there are concerns that system is going to be silo. Therefore WoT that makes IoT and applications work together, using the Web technology which does not depend on any frameworks is getting attention [1]. However, WoT servers need to be located on the Internet of global addresses, and the servers are always exposed to threats such as DDoS attacks. In 2016, Mirai [2], a malware, exploded on IoT devices. This has revealed the vulnerability of IoT devices. Since then, new types of malware countermeasures have been studied. In this paper, we propose a system to set a WoT server in a private address network and realize the direct communication between the WoT server and clients in the different private address networks by using NTMobile [3] [4]. According to this method, all the things that make up WoT can be set in the private address areas, and can be protected from external attacks.

As for verification, a RaspberryPi is used for the WoT server and extended to RC Tank (Hereafter, RasPiTank) [5]. We have confirmed that image communication and motor controls are possible by the proposed method. After this,Chapter 2 describes the related work, and chapter 3 describes the proposed method,and Chapter 4 describes verification, Chapter 5 describes evaluation, Finally, Chapter 6 concludes.

II. Related work

If you want to communicate directly between end nodes in the private networks, there is the way to use the WebRTC (Web Real-Time-Communication) technology [6]. WebRTC provides a method for end-to-end communication between clients connected to private networks by using ICE and other NAT traversal technologies. However, WebRTC has a problem that it is very difficult to construct the Web system required for WoT because it is specialized in the communication of video and voice.

OpenVPN (Open Virtual Private Network) [7] does not require kernel space operations, and can be used on various operating systems. However, it is necessary to consider that the addresses used by the applications and the addresses of the real networks do not overlap.

III. Proposed method

A. Outline of NTMobile

NTMobile assigns a virtual IP address independent of a real network, and a specific FQDN to an end node based on the account name and its password, or the certificate of the end node. This FQDN can be assigned in the form like "*.ntm.*". Therefore, it can be easily identified as an NTMobile terminal.

Fig. 1 shows the configuration of NTMobile. DC(Direction Coordinator) distributes the virtual addresses to all end nodes, and directs the communication route to both end nodes at the beginning of the communication. In the case when both end nodes are connected to different private address networks, or when they are connected to IPv4 and IPv6 networks, respectively, RS (Relay Server) is used to relay the communication packets. However, in the certain case of IPv4 communication, it is possible to carry out end-to-end communication without passing through RS by performing the NTMobile route optimization. In actual communication, the virtual IP address packets are encapsulated by the real IP address. This scheme enables NAT traversal and IP mobility.

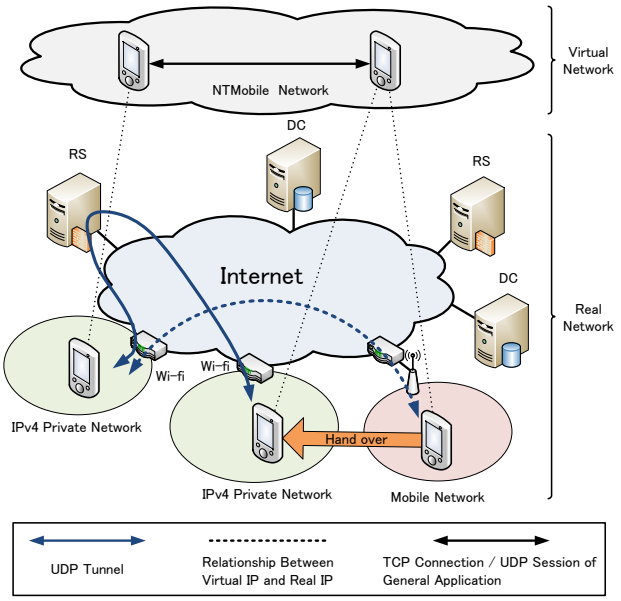

Fig. 1. Configuration of NTMobile

NTMobile uses the range "198.18.0.0/15" as the virtual IP addresses. This address range is defined for documentation by IANA [8], and does not overlap with real addresses.

NTMobile has been realized by various methods, such as the TUN usage type for LINUX, the built in library type for Linux application, the kernel type directly implemented in the Linux kernel, and the VpnService type for Android [9], and the operation verification has been completed.

B. Proposed System

The proposed method uses TUN-type NTMobile. This type of implementation allows general user programs to run on NTMobile, simply by starting the NTMobile application. Since TUN, which is a virtual interface, relays all user packets, existing user programs can work without any modification, and kernel modification is also not needed. That is, the WoT server and the client can be set in different private address networks, and they communicate each other as if the server is on the Internet. This method makes it possible to protect WoT servers from attacks such as DDoS attacks.

Although the proposed method, depending on the type of NATs, the communication route becomes via RS, however, it is more resistant to various attacks than the conventional WoT system configuration because RS has the following features.

- Since RS just relays packets, the execution cost is small.
- NTMobile discards unauthenticated packets immediately by our original way.
- RS can be located distributedly, and the load can be separated.

IV. Verification

The network configuration used in the verification is shown in Fig. 2. In the verification work, NTMobile communication

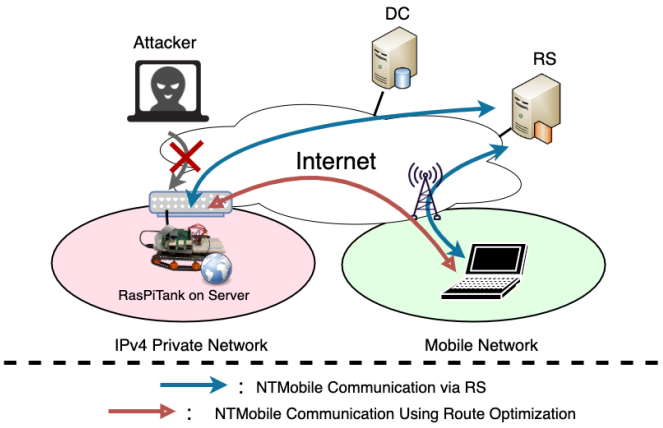

Fig. 2. Network configuration used in verification

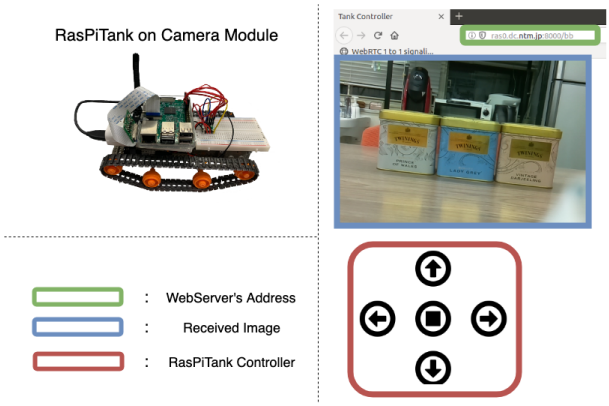

Fig. 3. External view of the Rasppie tank and browser operation screen

between end nodes is via RS. RasPiTank is connected to the IPv4 private network, and the laptop PC is connected to the Mobile Network by connecting WiMAX2. DC and RS were constructed in VPS of Ablenet, a cloud service. The RasPiTank used in the verification was constructed by connecting a camera module, an RC Tank extension kit, and a mobile battery to the RaspberryPi3ModelB. We used WebIOPi to build a web server in RasPiTank. WebIOPi enables to manipulate the GPIO pins of RaspberryPi from the client browser. We have developed the control program of the motor, and the image transfer from the camera of RaspberryPi as a web program. This program makes it possible to control the motor connected to the GPIO pin while checking the camera image shown on the browser screen.

Fig. 3 shows the RasPiTank connecting the camera module, and the layout of the client's web page. You can enter the FQDN of NTMobile specific assigned to RasPiTank and the port number of the application in the URL field of the browser. Then, an image taken by RasPiTank camera and the picture of arrows is displayed on the browser screen in order to control the motor.

V. Evaluation

Table I shows the comparison between the conventional technologies, WebRTC and OpenVPN, and the proposed

method, TUN type NTMobile. In terms of ease of implementation, WebRTC is set to Bad because it is necessary to incorporate the WebRTC library when creating an application. In the existing network item, OpenVPN is Fair because it may have to change the addresses of the existing networks. OpenVPN and TUN type NTMobile can use the network as they are. Regarding the items of applicable OS, WebRTC and OpenVPN are applied to many OSes. TUN type NTMobile is set to Fair Because which is currently only Linux, however, since it can be applied to Android, iOS and Windows in principle, it will be Good in future.

TABLE I
COMPARISON WITH RELATED WORK

	WebRTC	OpenVPN	NTMobile
Easy implementation	Bad	Good	Good
Existing network	Good	Fair	Good
Applicable OS	Good	Good	Fair

In the environment shown in Fig. 2, we have measured the packet transfer time from the PC connected to the mobile network to RasPiTank in the private network conneted by wire, via RS on the Internet. The specifications used for the measurement are shown in Table II.

TABLE II
SPECIFICATION OF EACH EQUIPMENT.

	OS	CPU	Memory
WebServer	Raspbian 9.11	Cortex-A53 4 Core 1.2GHz	1GB
Client	Ubuntu16.04LTS	Intel Corei5-2520M 2.5GHz	2GB
DC	CentOS 6.9	Virtual CPU 1 Core 3.3GHz	512 MB
RS	CentOS 6.9	Virtual CPU 2 Core 3.1GHz	1536 MB

The average value of 10 times was 95.22 [msec]. This value is not a problem in normal communication.

VI. CONCLUSION

In this paper, we have proposed the method to set a WoT server in a private address area by using NTMobile. As for verification, we constructed a web server using WebIOPi on RaspberryPi and set it in a private network, and confirmed that it can be controlled from a web terminal connected to Mobile Network.

REFERENCES

[1] World wide web consortium. https://www.w3.org/.

[2] Krebsonsecurity hit with record ddos. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[3] K. Naito, K. Kamienoo, T. Nishio, H. Suzuki, A. Watanabe, K. Mori, and H. Kobayashi. Proposal of seamless ip mobility schemes: Network traversal with mobility (ntmobile). In *Proc. of the IEEE Global Communications Conference (GLOBECOM 2012)*, Dec. 2012.

[4] H. Suzuki, K. Naito, K. Kamienoo, T.Hirose, and A. Watanabe. Ntmobile: New end-to-end communication architecture in ipv4 and ipv6. In *Proc. of the Proc. of ACM MobiCom 2013*, pp. 171–174, Oct. 2013.

[5] Streamtechnology - raspitank. https://www.streamtechnology.co.jp/RasPiTank/.

[6] Webrtc home — webrtc. https://webrtc.org/.

[7] Openvpn: Vpn software solutions & services for business. https://openvpn.net/.

[8] Rfc 2544 - benchmarking methodology for network interconnect devices. https://tools.ietf.org/html/rfc2544.

[9] T. Yamada, H. Suzuki, K. Naito, and A. Watanabe. Ip mobility protocol implementation method using vpnservice for android devices. In *Proc. of The 9th International Conference on Mobile Computing and Ubiquitous Networking (ICMU2016)*, pp. 67–68, Oct. 2016.