Host Migration Transparency Architecture by Cooperation between Multipath Transmission Control and VPN

1st Kohta Ohshima
Tokyo University of Marine Science and Technology
Tokyo, Japan
kxoh@kaiyodai.ac.jp

2nd Takehiko Kashiwagi
parallel networks LLC.
Tokyo, Japan

3th Yosuke Yano
iD corporation
Hokkaido, Japan

4rd Naoya Kitagawa
National Institute of Informatics
Tokyo, Japan
kitagawa@nii.ac.jp

***Abstract*—In this paper, we describe the basic design of network architecture with host mobility transparency for terminals equipped with multiple network interfaces. The features of the design are hardware acceleration using FPGA, functions to monitor and manage wireless connections, and the use of VPN to achieve both host migration transparency and seamless handover. We developed a prototype system and showed that it was possible to achieve host mobility transparency on the proposed architecture.**

***Index Terms*—host migration transparency, handover, Internet, VPN, mobility, multipath communication**

I. Introduction

Terminals equipped with multiple communication devices, e.g., smartphone and PCs, are increasing and there is a demand for continuity of communication using IP for mobile users. The problem of mobility in IP is that the address changes when the connected network changes due to movement. If the address changes during communication, a communication breakdown occurs and the terminal must be reconnected to continue communication. As a method of mobility support in IP environment, many methods of promptly notifying a new address to the source/destination terminal when an address changes, represented by Mobile IP [1], have been proposed. These methods are mainly intended for mobile terminals equipped with one network interface. Multipath TCP [2] is a protocol for improving the stability of communication in a terminal equipped with multiple network interfaces. Multipath TCP extends TCP to achieve increased bandwidth and fault tolerance by sending packets simultaneously using multiple paths. This method can be expected to have the effect of continuing communication even when moving, however using a Virtual Private Network (VPN) together may cause performance degradation due to the TCP-over-TCP problem.

This paper describes basic design of network architecture with host mobility transparency for terminals equipped with multiple network interfaces. The proposed architecture realizes a seamless handover that does not occur communication performance degradation and interrupt the communication session even when the address changes due to movement, while performing encrypted communication to ensure security.

II. Overview of Proposed Network Architecture

Figure II illustrates the proposed host migration transparency network architecture for multiple network interface environment. This architecture is constructed by terminals and routers. Terminals are information devices (PCs, smartphones, microcontrollers, etc.,) that can connect to the Internet via a gateway. Routers act as network gateways that enable site-to-site VPN connections, and also provide host migration transparency according to flow controller and connection controller. Flow controller has a function to manage and control how packets are distributed on multiple network interfaces. Distributing packets to multiple network interfaces can realize redundancy by copying packets, improvement of communication speed by round-robin transmission manner. However, when transmitting a large number of packets, the processing load becomes a bottleneck, and sufficient performance may not be obtained.

Our proposed architecture solves this problem using Field Programmable Gate Array (FPGA) hardware acceleration. Connection controller consists of the functions of monitoring wireless connection status and maintenance wireless connection. In this architecture, the router on the mobile side always establishes multiple wireless connections, and the wireless controller and flow controller work together to control at least one wireless connection to be in the connected state at all times. For example, when the signal strength of one wireless connection decreases, flow control is performed so that the other wireless connection is mainly used for communication, and the wireless connection whose signal strength has decreased is switched to a new connection. This operation allows the disconnect and reconnect delay times to be ignored. Reducing network switching time is important as it directly relates to QoS. A site-to-site VPN connection provides an encapsulation function that fixes the IP addresses between terminals even if the IP address on the Internet side of the router changes due to movement. Flow control and VPN can

 ISBN: 978-1-68558-052-0

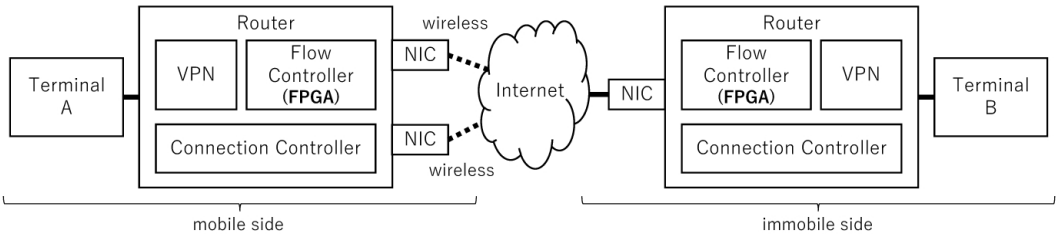

Fig. 1. Overview of the proposed network architecture

realize seamless handover function without adding functions to terminals.

III. Prototype Implementation and Evaluation

A. Prototype System

To verify that the host migration transparency feature of the proposed architecture works as intended, we developed a prototype system. This prototype system was developed using software and a wireless network interface, in order to confirm the effectiveness of the proposed architecture prior to implementation using FPGA,

Table I shows the specifications of the prototype system.

TABLE I
Specifications of the Router

Item	*Spec*
OS	Ubuntu 20.04 LTS
Wireless type	IEEE 802.11a
VPN	OpenVPN 2.54

B. Evaluation

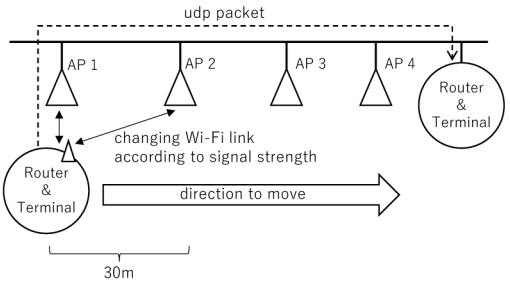

Fig. 2. Configuration of the evaluation environment

We conducted an evaluation experiment to confirm whether the proposed architecture can achieve host migration transparency. Figure 2 illustrates the evaluation environment. We evaluate host migration transparency and network reconnection latency by implementing a UDP packet transmitter in the mobile terminal that periodically sends UDP packets every 5 ms from the mobile terminal to the immobile terminal.

To evaluate the host migration transparency of this architecture, we used two different connection control methods: one that sets the SSIDs of all Wi-Fi Access Points (APs) the same and one that sets the SSIDs of all Wi-Fi APs to different names. Both connection control method automatically connects to nearby APs with stronger signal strength when the signal strength with the connected Wi-Fi AP become weak. The former aggressively switches connections, and the latter tries to maintain ongoing connections as much as possible. These connection controls are used standard Linux functions in this experiment.

As a result, the terminal was able to continue communication even after switching the connected network due to movement. In the same SSID case, about 600 packets were lost when network switching occurred. The time it takes to complete switching is about three seconds because one packet is sent every 0.5 ms. In the different SSID case, about 3,600 - 5,900 packets were lost when network switching occurred, and network switching delay is 19 - 30 seconds.

IV. Conclusions

In this paper, we described a basic design of network architecture with host mobility transparency for terminals equipped with multiple network interfaces. The proposed method is characterized that communication can be continued even if the terminal moves in the network, and the hardware acceleration of packet processing by FPGA. As a result of evaluating the mobility transparency of the proposed method, it was found that although the communication could be continued even if the network connection changed, the communication interruption time changed depending on the connection control method. In the future work, we will apply FPGA and implement and evaluate seamless handover method using multiple established wireless connections. And we will develop a communication stability improvement method that uses two or more wireless communications at the same time.

Acknowledgment

This work was supported by JKA and its promotion funds from KEIRIN RACE, and supported in part by JSPS KAKENHI Grant Number 22K12008.

References

[1] C. Perkins, “IP Mobility Support for IPv4,” RFC 3344, IETF, Aug. 2002.
[2] A. Ford, C. Raiciu, M. Handley, O. Bonaventure, and C. Paasch, “TCP Extensions for Multipath Operation with Multiple Addresses,” RFC 8648, IETF, Mar. 2020.

 ISBN: 978-1-68558-052-0