PMIPv6 빠른 핸드오버에서의 Out-of-Order 패킷 분석

Anh Khuong Quoc, 손민한, 추현승
성균관대학교 정보통신대학
e-mail : {kqanh, minari95, choo}@skku.edu

Out-of-Order Packet Analysis in Fast Handover for Proxy Mobile IPv6

Anh Khuong Quoc, Min Han Shon, and Hyunseung Choo
College of Information and Communication Engineering, Sungkyunkwan University

Abstract
Fast Handover for Proxy Mobile IPv6 (FPMIPv6), a protocol described in RFC 5949, is used to reduce handover latency and minimize packet loss problem occurring in the Proxy Mobile IPv6 (PMIPv6) protocol. However, during the study of implementing FPMIPv6, we found the Out-of-Order Packet (OoOP) problem that occurs in the experiment of PMIPv6. Since the OoOP is an issue that affects significantly to QoS of the network, in this paper, we analyze the OoOP problem by using network model. The analysis conducts the cause of occurring OoOP problem due to there exist two paths for data transmitted from Correspondent Node (CN) to MN in PMIPv6.

1. Introduction

In Wireless Networks (WNs), when an MN moves to the new location, the MN needs to change its IP address that affects to existing connections because the old IP address is no longer valid. This change in the IP address should be notified to the sender. With many MNs, the IP address changes affects to handover latency of application layer and increasing traffic load. To solve this mobility problem, we consider the network with the IP mobility support. Mobile IPv6 (MIPv6) [1], a host-based mobility management protocol developed by Internet Task Force (IETF), is proposed to enable IP services in the environment of mobile IP network. However, the Mobile Node (MN) of the MIPv6 is required to support the mobility protocol stack for handling the IP mobility. The MN awareness of the mobility makes the deployment of MIPv6 in practice to be inefficient.

Proxy Mobile IPv6 (PMIPv6) [2] is the protocol which has been standardized by Internet Engineering Task Force (IETF). It is also known as a network-based mobility management protocol which can enable IP mobility for MN without requesting the MN to take part in any mobility-related signaling. On behalf of the MN, the network responds for managing IP mobility, therefore, IP mobility is provided to any MN which is a node that does not run any mobile IP stack. However, the limitation of the current PMIPv6 is that its handover latency is still long and cannot prevent packet loss during the handover period.

The important of the mobility management is to provide the ongoing session and avoid the packet loss in communication between an MN and a correspondent node (CN) when the MN roams into the PMIPv6 domain. The Internet Engineering Task Force (IETF) developed the fast handovers for Proxy Mobile IPv6 (FPMIPv6) [3] to outperform the continuous service in PMIPv6 domain. However, FPMIPv6 does not consider about the OoOP problem that occurs because FPMIPv6 maintains two paths for data delivery from CN to MN at the time when MN has just attached to new Mobile Access Gateway (MAG). In the network environment and service provider, the OoOP problem causes losing the data at applications using the UDP protocol or the increase retransmission of the TCP protocol that reduces the overall network performance or the QoS of network.

The remainder of this paper is organized as follows. In section 2, we discuss existing related works, in which, we introduce the operation in FPMIPv6. In section 3, we analyze the OoOP problem using network model. Section 4 concludes this paper and briefly introduces the future work.

2. Related Work

FPMIPv6 is proposed to deal with the handover latency and packet loss issues when an MN roams in PMIPv6 domain by using the proactive approach. Fig 1 shows the signaling operation in FPMIPv6. First when Received Signal Strength (RSS) of the MN with the pMAG falls below the threshold, it scans neighboring MAGs to find the nMAG, from which the MN receives the strong RSS. The MN then sends the L2 report message that carries its ID and the nMAG address to the pMAG. Upon receiving the report
message, the pMAG start performing the handover initiate procedure to establish a bi-directional tunnel between the pMAG and the nMAG by sending the Handover Initiate (HI) message that carries the MN’s context to the nMAG. When the nMAG receives the HI message, it creates the tunnel with the pMAG and prepares for buffering data packets. After the tunnel is established, pMAG forwards data packets for MN to the nMAG through the tunnel, and then the nMAG buffers the data to avoid packet loss during MN handover period. When the MN attaches to the nMAG’s network, it broadcasts a Router Solicitation message that carries its MAC address or its ID to sense its presence in the new network. Once receiving the RS message from the MN, the nMAG flushes the buffered data packets to the MN before it sends PBU message to register MN’s information. Then, the nMAG starts performing procedure to register MN’s information by sending PBU message to the LMA according to PMIPv6 protocol.

![Signaling in FPMIPv6](image)

(Fig 1) Signaling in FPMIPv6

FPMIPv6 performs proactive handover by predicting the MN’s handover based on the RSS to prepare handling the handover before it happens. FPMIPv6 can avoid the packet loss by performing handover initiate to forward data packets for the MN from the pMAG to the nMAG if not, such packets will be lost during the period when the MN roams to the nMAG. In addition, the nMAG is aware of the MN’s information and prepares for the attachment’s the MN, therefore the nMAG performs flushing data packets as soon as MN’ attachment. It means that reducing the handover latency that is mentioned in [4].

3. Out-of-Order Packet analysis

FPMIPv6 performs a handover of an MN efficiently by reducing the handover latency and minimize the packet loss. Therefore we implement FPMIPv6 to bring it to practical. In the FPMIPv6 testbed, the statistic of data that we obtain by doing experiment for handover’s the MN proves that the handover latency is reduced impressively and packet loss almost is eliminated. However by analyzing the data, we reveal that there are a significant number of packets arrive at the MN in out-of-order. Fig 2 shows the OoOP problem in the testbed. In the fig 2, sending rate from Corresponding Node (CN) to MN $\lambda_s$ equals to 256 Kbps, and flushing rate from the nMAG to the MN $\lambda_f$ equals to 5x256 Kbps. We can see when MN attaches to the nMAG, the packets arrive at MN in out-of-order.

![Out-of-Order packets in FPMIPv6](image)

(Fig 2) Out-of-Order packets in FPMIPv6

The paper uses network model to analyze the OoOP problem. Figs 3, 4, 5 and 6 show a sequence images to describe the handover and express the OoOP problem in FPMIPv6. At first, during the movement of MN from the pMAG to the nMAG, the data packets from the CN to the MN are forwarded to and buffered at the nMAG via tunnel 1 and tunnel 2 as fig 4. Once the MN attaches to the MAG’s network, the nMAG flushes the buffered packets to the MN and then sending PBU and receiving PBA messages to and from the LMA to establish tunnel 3 as in Fig 5.

![FPMIPv6 operation: MN moves to nMAG](image)

(Fig 3) FPMIPv6 operation: MN moves to nMAG

When tunnel 3 is ready, the LMA change the route in routing table for packets delivered to the MN. Thus, the route now is changed from the old path that packets are delivered to the nMAG via tunnel 1 and tunnel 2 to the new path that packets delivered directly to the nMAG via the tunnel 3. Suppose that the sequence packets $S = \{P_1, P_2, ..., P_{i-1}\}$, in which $P_{i-1}$ is the last packet, are delivered via the old path, and the sequence packet $S' = \{P_i, P_{i+1}, ..., P_n\}$, in which $P_i$ is the first packet, are delivered via the new path as in fig 6. It
is obvious that the first portion of packets \( \{P_i, P_{i+1}, \ldots, P_n\} \) are delivered to the nMAG before the last portion of packet \( \{P_1, P_2, \ldots, P_{i-1}\} \), therefore the OoOP problem occurs when the packets arrive to the MN.

(Fig 4) FPMIPv6 operation: sending PBU and receiving PBA messages

(Fig 5) FPMIPv6 operation: Tunnel 3 is established

The degree of OoOP is depend on the parameters sending rate that is the speed of sending packets from CN to MN, link delay of the old path exclusive the new path, the delay of the attachment at link layer and the flushing rate that is the speed of forwarding buffered packets. The degree of OoOP is increased if the parameters sending rate, exclusive link delay and the delay at link layer are larger and the parameter flushing rate is smaller. In the contract, if the parameters sending rate, exclusive link delay and the delay at link layer are smaller and the parameter flushing rate is larger, the number of Out-of-order packets are decreased.

(Fig 6) FPMIPv6 operation: Out-of-order packets

In our testbed, we measure the impact of these parameters by do the experiment of FPMIPv6 implementation in different parameters such as sending rate that is the speed of sending packet from the CN to the MN and flushing rate that is the speed of sending buffered packet from the nMAG to the MN. The result in the testbed and the mathematic analysis demonstrates the impact of OoOP problem in FPMIPv6.

4. Conclusion
When implementing FPMIPv6, we real the out-of-order packet problem in the testbed. Since the problem affects significantly to the QoS of network and quality of services, we analyze the OoOP problem by network model to evaluate the number packets in out-of-order when MN performs a fast handover in PMIPv6. For the future work, we will propose a new scheme to solve OoOP problem in FPMIPv6 scheme and implement the new scheme in the testbed to evaluate the performance.

ACKNOWLEDGMENT
This research was supported in part by MSIP(NIPA,KEIT) and MOE(NRF), Korean government, under ITRC (NIPA-2013-(H0301-13-3001)), IT R&D Program[10041244, SmartTV 2.0 Software Platform], and PRCP(NRF-2010-0020210), respectively.

References