The Reliable Packet Transmission Based on PMIPv6 Route Optimization

NamYeong Kwon
School of Information and Communication Engineering
Sungkyunkwan University
Suwon, Korea
nykwon@skku.edu

Moonseong Kim
Korean Intellectual Property Office
Daejeon, Korea
moonseong@kipo.go.kr

Seung-Tak Oh
School of Information and Communication Engineering
Sungkyunkwan University
Suwon, Korea
xrossat@ece.skku.ac.kr

Hyunseung Choo
Department of Interaction Science
Sungkyunkwan University
Suwon, Korea
choo@ece.skku.ac.kr

Abstract— **Route Optimization (RO) is a function to minimize packet transmission delay through the optimal path between routers communicating with each other. Mobile IPv6 (MIPv6) also supports the RO to solve the triangle routing problem. Basic PMIPv6 does not support the RO. Thus, many schemes have been proposed to support RO in PMIPv6. However, these schemes do not consider the out-of-sequence problem, in which packets arrive out of order, which may happen between the existing path and the newly established RO path. This paper proposes a scheme to solve the out-of-sequence problem more precisely and with low cost. Our proposed scheme solves the problem by using the packet sequence number and the time when the problem occurs. In this paper, we compare PMIPv6 supported by the RO and the Out-of-sequence Time Period (OTP) scheme with our proposed scheme via simulation. Evaluation of the performance reveals PMIPv6 supported by the RO had 66 of out-of-sequence packets, and the OTP scheme has 30. However, our proposed scheme does not incur out-of sequence packets. Our proposed scheme guarantees reliable packet transmission by preventing the problem.**

Keywords- PMIPv6, Proxy Mobile IPv6, RO, Route Optimization, Out-of-sequence, Out-of-order

I. INTRODUCTION

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol that supports network mobility, regardless of whether or not a Mobile Node (MN) supports mobility protocol [1]. This particular feature enables resource optimization in their networks and reduces energy consumption of an MN and handover signaling cost. A Mobile Access Gateway (MAG) and a Local Mobility Anchor (LMA) are in charge of the mobility of an MN in the PMIPv6 domain. However, basic PMIPv6 does not support Route Optimization (RO). If so, all packets are always transmitted via an LMA, and this increases the load of an LMA and increases packet transmission delay. Many schemes are proposed to support the RO to resolve this problem in PMIPv6 [2].

When the RO occurs in PMIPv6, the MN communicates with the Correspondent Node (CN) via the RO path between MAGs. In this paper, we define the RO path as a new path, and the basic PMIPv6 path as an old path. When the new path is established, the out-of-sequence problem occurs due to the difference the transmission time between the old path and the new path. This problem causes packet loss in User Datagram Protocol (UDP) and packet retransmission request messages in Transmission Control Protocol (TCP). The Out-of-sequence Time Period (OTP) [3] scheme is proposed to resolve the problem. The OTP scheme is the solution to restrain the tunnel establishment when the new path is established. However, the scheme cannot provide reliable service to an MN, because it is hard to predict the restraint time of the tunnel establishment in the OTP scheme.

In this paper, we propose the scheme to solve the out-of-sequence problem that is more accurate and effective. Our proposed scheme resolves the problem using the identical sequence number of a packet and uses the original RO control message of PMIPv6 supported by RO. Our proposed scheme precisely prevents the problem compared to the OTP scheme, since it uses the sequence number. In addition, it reduces the buffering cost by reducing the number of entities performing the buffering.

The remainder of this paper is organized as follows. Section 2 introduces the OTP scheme. Section 3 illustrates the basic assumptions of our proposed scheme, basic algorithm, and signaling flow. Section 4 evaluates the simulation of the number of out-of-sequence packets and the handover delay. Section 5 concludes the paper and outlines our future work.

II. PREVIOUS WORK

The RO schemes for PMIPv6 have been proposed. The packets generated between an MN and a CN are transmitted via an LMA before the new path is created. After the RO, a tunnel is established between the MAGs that the MN and the CN are

*Corresponding Author: H. Choo

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

connected. However, tunnels exist in the old path and the new path. Some packets are transmitted using the old path and some packets are transmitted using the new path. Therefore, the out-of-sequence problem occurs. The OTP scheme was proposed to prevent this problem.

The OTP scheme solves the problem using the different times to establish between the old path and the new path. The scheme uses the time to predict the terms of incurring the out-of-sequence packet and the amount of buffered packets. The scheme stores all of the packets in the MAG and the LMA when the binding update is completed. The packets transmitted from MN to CN are stored at MAG connected to MN, and the packets transmitted from CN to MN are stored at the LMA connected to CN. After the new path is established or if the RO Report message does not arrive at the LMA during the OTP time, MAG and LMA forward the buffered packets to each destination.

The OTP scheme prevents the problem by the tunnel restraint during the RO in PMIPv6, but it stores the packets at both MAG and LMA. In addition, it does not forward the packet during the RO. Therefore, the packet reception delay is longer than the PMIPv6 supported by RO. It predicts the tunnel restraint time to resolve the problem, but the approach to the prediction does not guarantee prevention of out-of-sequence packets precisely.

III. PROPOSED SCHEME

Our proposed scheme provides the reliable service for an MN more accurately to prevent the out-of-sequence problem. Our proposed scheme resolves the problem effectively, using the packet sequence number, and reducing the forwarding delay time using the value of Time To Live (TTL).

A. Motivation and Basic Assumptions

In our proposed scheme, only MAG performs the buffering for MN so the buffering cost in LMA decreases, whereas both the MAG and the LMA in the OTP scheme. In addition, the OTP scheme does not perfectly prevent the problem due to the prediction. However, our proposed scheme prevents the problem perfectly, using the packet sequence number. In this paper, we assume that the MN sends some packets to CN after an MN's handover to explain this more effectively.

We use the IP header's information to prevent the problem more effectively [4]. The identification field, which is the number assigned from a router of the IP header, is a unique number used by devising or recombining a packet following the Maximum Transfer Unit (MTU). Accordingly, it is possible to know the packet sequence using the identification number in the communication between routers. MAGs and LMAs know the packet sequence via the identification number in the IP header. Therefore, our proposed scheme determines the out-of-sequence packets that arrive at the MAG by the identification number in the IP header.

Our proposed scheme uses the TTL value in the IP header to calculate the transmission time of the old path and the new path. We count the number of routers through the old path and the new path from the TTL value. The TTL value in the tunnel header decreases when the packet passes through the tunnel, since the packet is encapsulated, but the TTL value in the IP header does not. The packet is decapsulated after passing through the tunnel. Then, the TTL value in IP header decreases just one [5]. It is impossible to count the accurate number of routers in each path due to this situation. Our proposed scheme uses the minimal encapsulation to resolve the problem [6]. Minimal encapsulation is proposed to reduce the header's overhead. The TTL value usually decreases after a packet passes through the tunnel, because the minimum information is kept at the inner IP header, and the remaining information moves to the tunnel header.

Our proposed scheme reduces the load of the router to minimize the number of routers that take the buffering. $Entity_{Node}$ is an entity connecting to a node. All of MAGs and an LMA perform the buffering in the case of the OTP scheme; however, our proposed scheme performs the buffering on the MAG_{CN}. When a packet arrives at MAG_{CN} through an old path, MAG_{CN} forwards the packet to CN. Conversely, if a packet goes via the new path, MAG_{CN} stores the packet in its buffer. Thus, our proposed scheme reduces the load of the LMA and packet reception delay of the CN.

B. Basic Operation

The procedure to establish the new path is similar to the scheme written by P. Loureiro and M. Liebsch [2]. The packets between an MN and a CN pass through the old path before the new path is established. If the new path is established, the packets pass through the new path. MAG_{CN} receiving the packets via the new path, buffers the packets to prevent the problem. From the beginning of the buffering in MAG_{CN}, MAG_{CN} compares the sequence number of the first packet in the buffer and the sequence number of the packet that passed via the old path. MAG_{CN} performs the buffering until the last packet from the old path arrives at MAG_{CN}. When the last packet from the old path arrives at MAG_{CN}, MAG_{CN} forwards the packet and then forwards the all packets in its buffer.

In our proposed scheme, the problem is prevented by storing the packets from the new path in the MAG's buffer, until all the packets pass from the old path. Enabling the sequence number to understand the order of all the packets passing though the old and new path resolves the problem more precisely than other schemes do. In addition, our proposed scheme transfers via the shortest path due to performing the buffering in $MAG_{CN,}$ Thus, the problem is resolved, and the packet reception delay is reduced.

MAG_{CN} forwards the packets in the buffer to CN after the last packet from the old path passes through MAG_{CN}. However, if the last packet from the old path is lost, MAG_{CN} performs the buffering infinitely. The maximum forwarding delay time (T_{wait}) is calculated to prevent infinite buffering in our proposed scheme. If the last packet from the old path does not arrive at MAG_{CN} within the T_{wait}, the packets in the buffer are forwarded to CN. The problem is prevented using the maximum forwarding delay time, even though the packets from the old path are lost.

$$T_{wait} = T_{OP} - T_{NP} \quad (1)$$

$$T_{OP} = \left(TTL_{Max} - TTL_{OP}\right) \cdot T_{One-Hop} \quad (2)$$

$$T_{NP} = \left(TTL_{Max} - TTL_{NP}\right) \cdot T_{One-Hop} \quad (3)$$

T_{wait} is calculated by the time difference between the times that the packets coming from the old path and the new path, arrive at MAG_{CN}. T_{wait} is calculated by equation (1). T_{OP} and T_{NP} define the time that the packet passes via the old path and the new path, respectively. From equation (1), we calculate the different arrival times between T_{OP} and T_{NP}. Equation (2) and (3) are the formulas to calculate T_{OP} and T_{NP}. TTL_{Max} is the maximum value of TTL. TTL_{OP} and TTL_{NP} are the TTL values of the packets from the old path and the new path, respectively.

$$T_{One-Hop} = \frac{L_{MTU} \cdot \frac{\left(\frac{T_{RS}}{2}\right)}{L_{RO-Setup}}}{TTL_{Max} - TTL_{RS}} \quad (4)$$

$T_{One-Hop}$ is calculated by equation (4). $T_{One-Hop}$ is calculated using the round-trip time and TTL value of the RO Setup message that sets up the new path. TTL_{RS} is the TTL value when the RO Setup message arrives at MAG_{CN}, and L_{MTU} is the MTU size. T_{RS} is the round-trip time of the RO setup message and $L_{RO\text{-}Setup}$ is the size of the RO Setup message. The transmission time of the old path, the new path, and the transmission time per hop are calculated using the RO Setup message.

C. Signaling of the Proposed Scheme

Fig. 1 shows the signaling flow of our proposed scheme when the last packet from the old path is lost in MN's inter-domain handover. When MAG2 receives the RO Init message from LMA2, MAG2 performs the flow to calculate the T_{wait}. MAG2 saves the TTL value of the RO Setup message and inter-arrival time of the RO Setup message between MAG1 and MAG2.

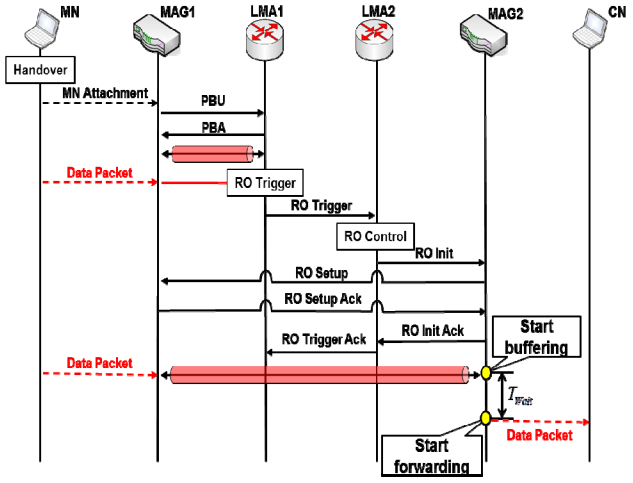

Figure 1. Signaling flow of the proposed scheme.

When the RO is completed, MAG2 starts to store the packets from the new path and checks the packet sequence number from the old path. If the last packet from the old path arrives at MAG2, MAG2 forwards the packet to CN. Next, MAG2 forwards all the buffered packets in MAG2 to CN. However, if the last packet from the old path does not arrive at MAG2 during T_{wait}, MAG2 determines the last packet from the old path is lost. Therefore, MAG2 forwards all buffered packets in its buffer to CN.

Our proposed scheme provides reliable service to resolve the out-of-sequence problem more precisely than the OTP scheme. The problem is prevented using T_{wait}, even though the packets from the old path are lost. In addition, the scheme minimizes the packet reception delay, using the old path during the establishment of the new path. Moreover, our proposed scheme reduces the buffering cost, because the buffering is performed only by MAG_{CN}.

IV. Performance Evaluation

In this section, we verify the number of out-of-sequence packets and the packet reception delay by simulation. Our proposed scheme generates fewer out-of-sequences than the OTP scheme and PMIPv6 supported by the RO. In addition, it demonstrates improved performance in terms of packet reception delay compared to the OTP scheme.

A. Experimental Environment

We run the simulator implemented in C++ to measure the number of the out-of-sequence packets. We conduct our experiment in the UDP environment to determine the packet loss and out-of-sequence packets. The experiment uses the CBR traffic generator, and data packets are generated in 0.02 seconds interval. If the traffic is generated by CBR, we verify the incidence of packet reception delay and the number of out-of-sequence packets accurately. Packet size is fixed at 500 bytes [7].

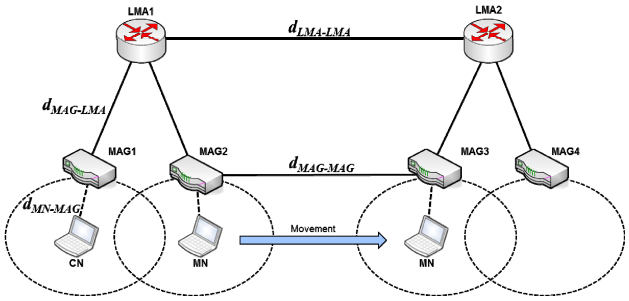

Figure 2. Network topology of simulation.

Fig. 2 is network structure to conduct the experiment. We configure $d_{LMA\text{-}LMA}$ as 15hops, $d_{MAG\text{-}LMA}$ and $d_{MAG\text{-}MAG}$ as 7hops, $d_{MN\text{-}MAG}$ as 1hop. In this experiment, the number of the out-of-sequence packets and the packet reception delay are verified during the RO setup in the inter-domain handover.

B. Simulation Results

Fig. 3 shows the simulation results of PMIPv6 supported by RO. This scheme cannot prevent occurrence of out-of–sequence packets. Fig. 4 shows the simulation results of the OTP scheme. Fig. 5 is the simulation results of our proposed

scheme. The results show the cases where the last packet from the old path are lost and not lost.

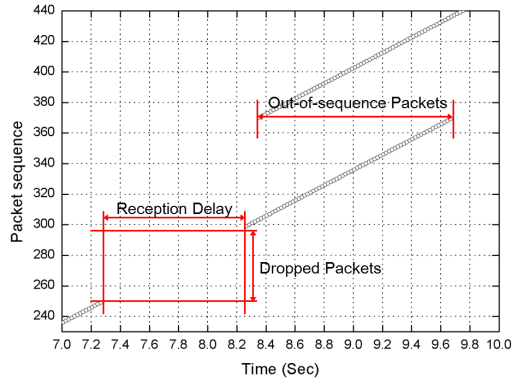

Figure 3. PMIPv6 support by RO.

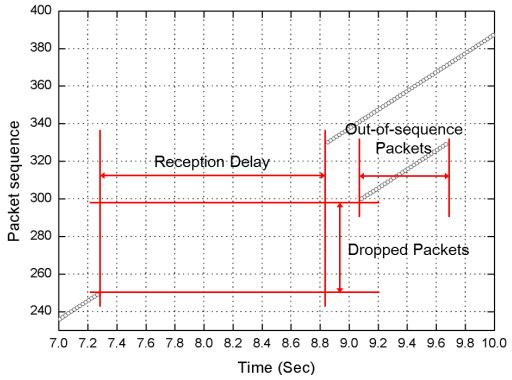

Figure 4. OTP scheme.

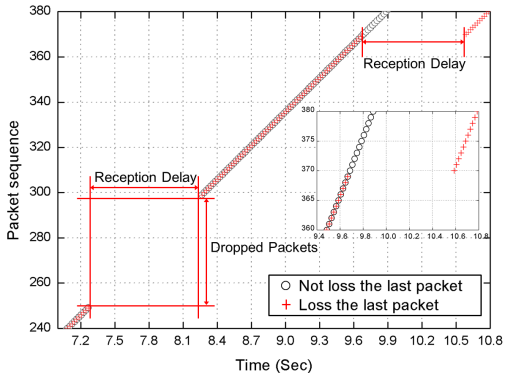

Figure 5. Proposed scheme.

TABLE I. SIMULATION RESULTS

Schemes	Out-of-sequence Packets	Dropped Packets	Packet Reception Delay
PMIPv6 supported by RO	66	49	0.947 sec
OTP Scheme	30	50	1.82 sec
Proposed Scheme (Not Loss)	0	50	0.947 sec
Proposed Scheme (Loss)	0	50	1.915 sec

Table 1 shows the simulation results of each scheme. The three compared schemes in the simulation incurred a similar number of lost packets, because they do not have a function to prevent packet loss. The OTP scheme decreases the packet loss compared to PMIPv6 supported by the RO, but it increases reception delay. However, our proposed scheme prevents all out-of-sequence packets. The packets lost and reception delay are the same as in PMIPv6 supported by RO. Even if the last packet from the old path is lost, the out-of-sequence packets will not occur. Our proposed scheme prevents the out-of-sequence problem and supports reliable service more effectively.

V. CONCLUSION

The difference of the transmission delay between the old path and the new path generates the out-of-sequence problem in PMIPv6. Some schemes are proposed to resolve the out-of-sequence problem, but they do not solve the problem effectively. Our proposed scheme provides reliable service for MN more accurately to prevent the problem occurring from the RO. The scheme resolves the problem effectively, using the packet sequence number, and reduces the forwarding delay time using T_{wait}.

In this paper, we compare PMIPv6 supported by RO and the OTP scheme with our proposed scheme via simulation. Our proposed scheme resolved the out-of-sequence problem and reduced the packet reception delay after the new path is established. We provide a reliable service in PMIPv6 RO by adapting our proposed scheme. We will evaluate the performance of our proposed scheme in the future using a test bed and mathematical modeling.

ACKNOWLEDGMENT

This research was supported by PRCP(2011-0018397), NICDP(2011-0020517), and WCU(R31-2010-000-10062-0) through NRF of Korea, respectively.

REFERENCES

[1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," IETF RFC 5213, 2008.

[2] P. Loureiro and M. Liebsch, "Proxy Mobile IPv6 Localized Routing," draft-loureiro- netext-pmipv6-ro-02.txt (expired), 2010.

[3] J. Lee, Y. Kim, and H. Lee, "Tunnel Restraint to Prevent Out-of-Order Packets for Route Optimization in Proxy Mobile IPv6," Wireless Personal Communications, vo.58, 2011.

[4] J. Postel, "Internet Protocol," IETF RFC 791, 1981.

[5] C. Perkins, "IP Encapsulation within IP," IETF RFC 2003, 1996.

[6] C. Perkins, "Minimal Encapsulation within IP," IETF RFC 2004, 1996.

[7] A. Udugama, M, U. Iqbal, U. Toseef, C. Goerg, C. Fan, and M. Schlaeger, "Evaluation of a Network based Mobility Management Protocol : PMIPv6," Proc. of IEEE 69th Vehicular Technology Conference, pp.1-5, 2009.