Context Reflector for Proxy Mobile IPv6

Sawako Kiriyama[1]*, Ryuji Wakikawa[2], Jinwei Xia[3] and Fumio Teraoka[1]
[1] *Keio University*
Yokohama, Kanagawa, Japan
{*kiri@tera.ics.keio.ac.jp* and *tera@ics.keio.ac.jp*}
[2] *TOYOTA InfoTechnology Center, U.S.A., Inc.*
Mountain View, CA., U.S.A.
ryuji@jp-toyota-itc.com
[3] *Huawei Technologies Co., Ltd.*
Nanjing, P. R. China
xiajinwei@huawei.com

Abstract

Proxy Mobile IPv6 has been standardized as a network-based mobility management protocol in the IETF. To optimize mobile node's handover performance, a context of the mobile node such as its identifier, accounting, authentication and authorization states is expected to be transferred between mobility entities. This paper proposes a simple context transfer mechanism named Context Reflector for Proxy Mobile IPv6 (Context Reflector). Context Reflector carries any kinds of information of mobile nodes. With Context Reflector, the service such as AAA (Authentication, Authorization, and Accounting), ROHC (Robust Header Compression) and QoS (Quality of Service) can be quickly re-established after handover of the mobile node. Therefore, the handover latency and the packet loss during handover can be reduced. Comparisons of Context Reflector and other approaches make it clear that Context Reflector is superior in terms of packet loss and handover latency during handover.

1 Introduction

Recently, ubiquitous Internet access becomes reality by the progresses of wireless technologies. A mobile node (MN) is capable of roaming to different wireless networks with movement transparency. To provide movement transparency, Mobile IPv6 (MIPv6) has been standardized as RFC3775[1] in the Internet Engineer Task Force (IETF) in 2004. Unfortunately, it is not deployed and available in the global Internet. One of the reasons of limited deployment is that MIPv6 requires modifications to the MN for mobility related signaling. Since the MN tends to equip only limited computational resources in a small terminal, these modifications and processing overheads are not always acceptable.

As a solution of this problem, a network-based mobility management protocol such as Proxy Mobile IPv6 (PMIPv6)[2] has been proposed. With PMIPv6, it is possible to support mobility for the MN without any modifications to the MN. The mobility entities in the network track the movement of the MN. They exchange all mobility related signaling and set up the required routing state for the MN. A couple of papers[3, 4] showed that PMIPv6 can reduce the handover latency in terms of the signaling procedure in comparison with Mobile IPv6. In an actual operation, the information called the context of the MN must be transferred from the current point of attachment to the next point of attachment in addition to signaling procedure when a handover occurs. This procedure is called *the context transfer*. However, PMIPv6 does not take into account context transfer.

This paper proposes a context transfer mechanism called *Context Reflector for Proxy Mobile IPv6* (Context Reflector, in short) as for optimizing handover process of PMIPv6. In Context Reflector, the

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 2/3, pp. 36-51
*Currently in Sony Corp.

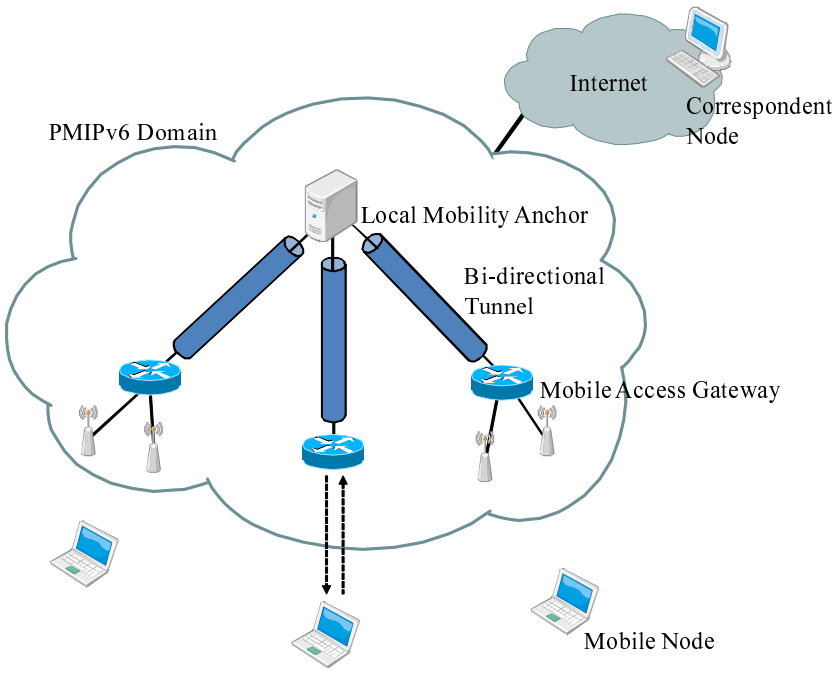

Figure 1: An example of network topology of PMIPv6

information (context) of the MN is transferred between the mobility entities in the network before the MN changes its attachment point. By this context transfer capability, the mobility entities are capable of controlling the data traffic of the MN to reduce packet loss.

The remainder of this paper is organized as follows. Section 2 describes an overview of PMIPv6 and its problems in handover optimization. We propose a simple context transfer mechanism named *Context Reflector for Proxy Mobile IPv6* to improve handover performance in PMIPv6 in Section 3. We also compare our proposed mechanism with other proposals in Section 4. Implementation and evaluation of Context Reflector for PMIPv6 are described in Section 5. We make a conclusion in Section 6.

This paper is an extended version of a paper presented in "The 3rd International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2009)"[5].

2 Proxy Mobile IPv6 and Problem Statement

2.1 Protocol Overview

Proxy Mobile IPv6 (PMIPv6) has been standardized as RFC5213 at the Network-based Localized Mobility Management (netlmm) Working Group in the IETF. The network where PMIPv6 is used for mobility management of the MN is called a Proxy Mobile IPv6 domain (PMIPv6-Domain) and the MN is provided with transparent communication while it is moving in the PMIPv6-Domain. In PMIPv6, the MN is assigned a Mobile Node's Home Network Prefix (MN-HNP) and configures a Mobile Node's Home Address (MN-HoA) from this prefix. The MN will be able to use the MN-HoA as long as it is in the PMIPv6-Domain. Additionally, the MN is identified by the Mobile Node Identifier (MN-ID) in the PMIPv6-Domain.

Figure 1 shows an example of network topology of PMIPv6. The core functional entities in PMIPv6 are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is a router that supports mobility for MNs. It allocates the MN-HNP to the MN and maintains the binding between

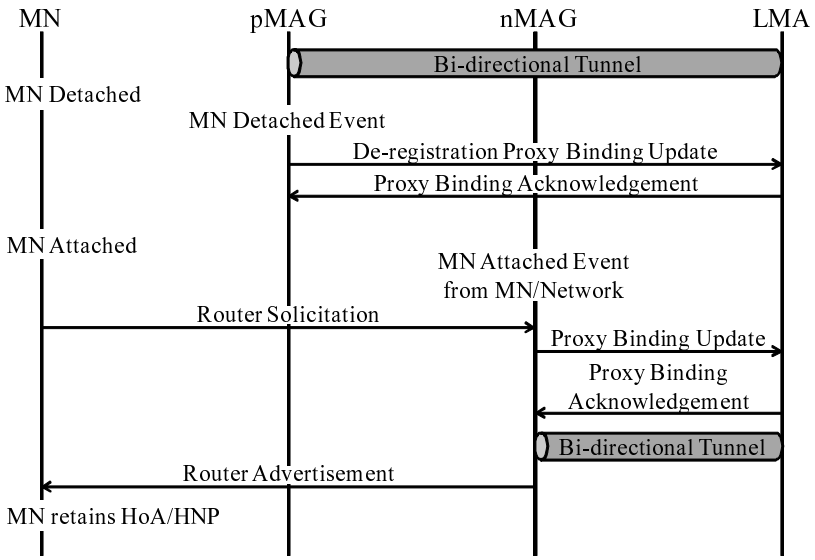

Figure 2: Signaling sequence of PMIPv6 handover

the MN-HNP and the Proxy Care-of Address (Proxy-CoA). The Proxy-CoA is the global address of the MAG to which the MN attaches. This binding is stored in the Binding Cache Entry (BCE) in the LMA. Additionally, the LMA is the topological anchor point for the MN-HNP, so that all the data traffic for the MN will be routed through the LMA. The MAG is an access router that manages mobility related signaling for the MN that attaches to its access link and acts as the default router for the MN. The MAG is responsible for tracking the movement of the MN and for signaling to the LMA of the MN. Moreover, a bi-directional tunnel, which is a secure tunnel by IPsec, is established between the LMA and the MAG, and all data traffic for the MN will be routed through this tunnel.

Figure 2 shows the signaling sequence of the handover of the MN from the previous MAG (pMAG) to the new MAG (nMAG). When the pMAG detects the detachment of the MN from the link, it sends the de-registration Proxy Binding Update (PBU) message to the LMA in order to request deletion of the BCE of the MN in the LMA. Upon receiving this request, the LMA stops forwarding of the data traffic of the MN and waits for a certain period of time before it deletes the BCE of the MN. If the LMA receives the PBU from the nMAG as a request to update the BCE of the MN during a certain period of time, the LMA does not delete it and updates the Proxy-CoA of the MN to the address of the nMAG. The LMA starts forwarding of the data traffic of the MN to the nMAG. Finally, the LMA sends the Proxy Binding Acknowledgement (PBA) message in reply to the PBU.

2.2 Problem Statement: Lack of Context Transfer Mechanism

When a MN attaches to a MAG, the MAG owns and manages plenty of states about the MN. The states of the MN are called the context and they include protocol states of PMIPv6, Authentication, Authorization and Accounting (AAA), Robust Header Compression (ROHC) and Quality of Service (QoS). These states are always required for the MN to connect to a PMIPv6-Domain. The typical context of PMIPv6 includes the MN-ID and the MN-HNP stored in the policy profile of the MN and the Proxy-CoA. This context is retrieved by the MAG before providing mobility service to the MN.

This context of the MN is dynamic and active, and is stored in the MAG only while the MN attaches to the MAG. Whenever a MN changes the attached MAG, the nMAG re-generates such context for the MN by re-running protocols such as AAA, ROHC and QoS from the beginning. For example, in

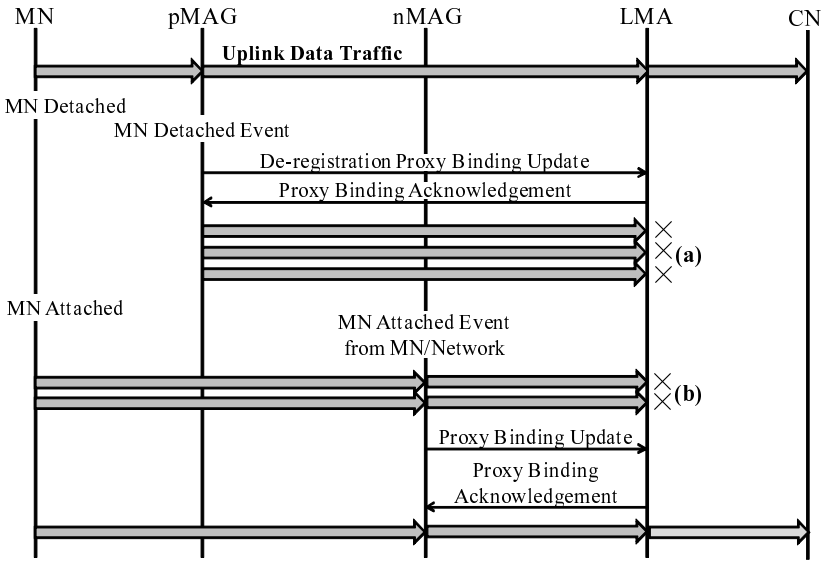

Figure 3: Uplink data traffic flow of the MN in handover of PMIPv6

Figure 2, when the MN changes the attached MAG from the pMAG to the nMAG, the nMAG starts sequences of AAA, ROHC and QoS if necessary. However, since the MN has been authenticated at pMAG before handover, this re-authentication is a somehow redundant operation. It causes severe packet loss and handover latency because the nMAG cannot send the PBU to the LMA before authentication (i.e., creating required context for the MN). RFC3374[6] explains the details of the problem statement in case without transferring the context of the MN for these services such as AAA, ROHC and QoS.

Without transferring the context of the MN, the MN might encounter tremendous packet loss. This problem is summarized in [7]. The uplink traffic flow of the MN in handover of PMIPv6 is shown in Figure 3. The bold arrows in the figure mean the uplink data traffic of the MN. When the LMA receives the de-registration PBU from the pMAG, it stops forwarding the uplink data traffic of the MN until it acquires the new Proxy-CoA by receiving the PBU from the nMAG. The pMAG might still have delayed the uplink data traffic of the MN after the detachment of the MN (Figure 3(a)). In Addition, since the address configuration of the MN-HoA has already been accomplished, the MN can send the packets as soon as it attaches to the nMAG. The uplink data traffic of the MN might be delivered from the nMAG before the operation by exchanging the PBU and the PBA is completed (Figure 3(b)). Therefore, the LMA cannot accept and route these uplink data traffic of the MN. Similarly, the LMA cannot accept and route the downlink data traffic of the MN after receiving the de-registration PBU from the pMAG until it receives the PBU from the nMAG. It is because that the LMA does not know the new Proxy-CoA, i.e., the destination to which the downlink traffic of the MN is forwarded. With transferring nMAG's address as the context of the MN, the LMA can acquire the new Proxy-CoA of the MN before the attachment of the MN to the nMAG and control the data traffic of the MN to prevent packet loss.

When the LMA receives the PBU from the nMAG, it updates the Proxy-CoA of the MN to the IP address of the nMAG. In PMIPv6, the LMA forwards only the uplink data traffic of which the source IP address matches the registered Proxy-CoA on the BCE of the MN. Therefore, the LMA cannot accept and route the delayed uplink data traffic of the MN sent from the pMAG after updating the Proxy-CoA of the MN.

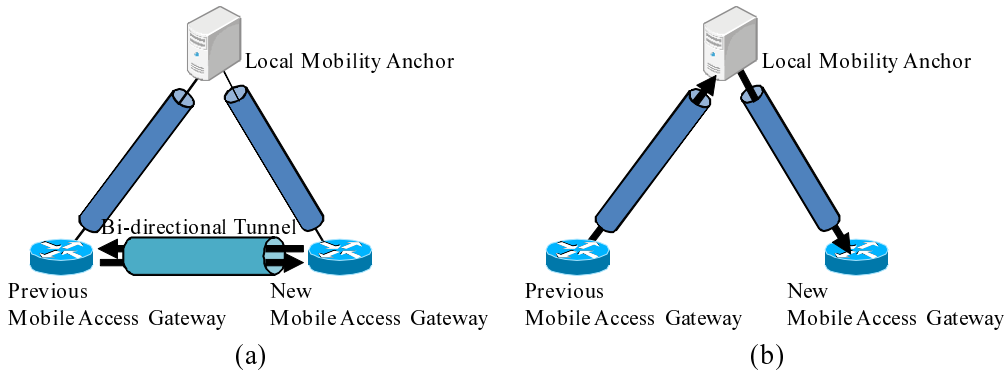

Figure 4: Comparison of the delivery paths of the context of the MN (a) between the two MAGs and (b) via the LMA in L3 topology

3 Context Reflector for Proxy Mobile IPv6

In the previous section, we described the importance of a context transfer mechanism, but a context transfer mechanism is not specified between a pMAG and an nMAG in PMIPv6. Therefore, we propose a context transfer mechanism named *Context Reflector for Proxy Mobile IPv6* (hereafter called "Context Reflector").

3.1 Design Approach

3.1.1 Approach to transfer the context of the MN

There are two prominent types of approaches to transfer the context of the MN. The first approach is that the context of the MN is transferred from the pMAG to the nMAG directly. Each MAG does not maintain any security association with other MAGs. Therefore, to transfer the context of the MN securely, each MAG must establish new security associations between all the MAGs to which the MN can move and attach. The overhead of trust establishments among all the MAGs is large and cannot be ignored. The second approach is that the context of the MN is transferred from the pMAG to the nMAG via the LMA. So, it is sent from the pMAG to the LMA and forwarded from the LMA to the nMAG. Therefore, the MAG needs only one security association to the LMA to transfer the context of the MN securely. Since each MAG has a certain security association with the LMA for the PMIPv6 operation, this approach does not need to establish a new security association. In addition, the LMA can also acquire the context of the MN before the MN attaches to the nMAG.

Figures 4 and 5 show examples of network layer (layer 3) and physical layer (layer 1) topology in PMIPv6. From the layer 3 topology viewpoint, the second approach (Figure 4(b)) has a longer path to send the context of the MN than the first approach (Figure 4(a)). However, if you see the layer 1 topology, it is not common to have a direct connection between the two MAGs. It is burden for operators to install the direct line among MAGs and maintain them. A MAG might be required to have direct path to plenty of neighboring MAGs. Even if the context of the MN is directly sent between the two MAGs from the layer 3 viewpoint, it is sent via a network core (where the LMA often locates). Consequently, we adopt the second approach, i.e., transferring the context of the MN via the LMA, as the method to transfer the context of the MN.

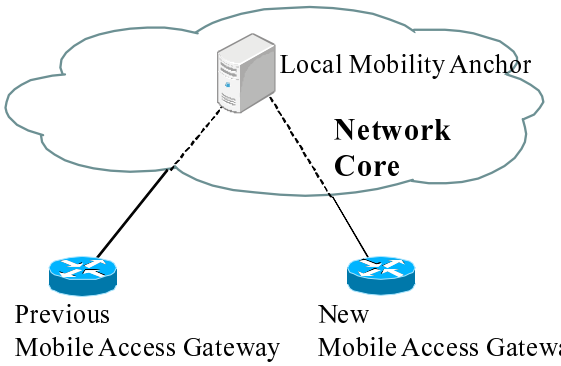

Figure 5: L1 topology of PMIPv6

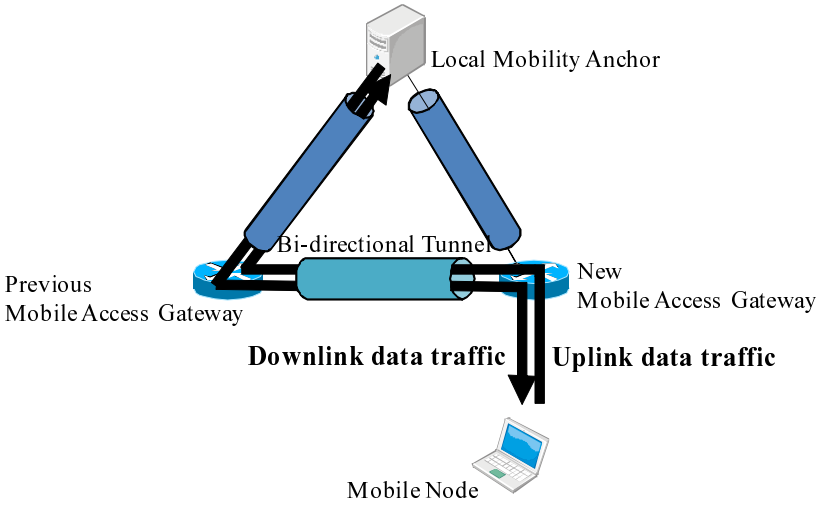

Figure 6: The delivery path of the forwarded the data traffic of the MN by the pMAG and the nMAG

3.1.2 Flow Management

To reduce packet loss during handover, the mobility entities in the network should control the data traffic of the MN. There are two prominent types of approaches of flow management. The first approach is that the pMAG and the nMAG control the data traffic of the MN. The pMAG and the nMAG know each other's IP address and forward the data traffic of the MN. Figure 6 shows the delivery path of the data traffic of the MN in this approach. As shown in this figure, the data traffic of the MN is delivered from/to the LMA and to/from the nMAG via the pMAG. Normally, it is delivered from/to the LMA and to/from the nMAG directly in PMIPv6. In this approach, since it is delivered via the pMAG, its delivery path is redundant. Additionally, to exchange the data traffic of the MN between the two MAGs, they need to establish a bi-directional tunnel and perform tunneling processing such as encapsulation and decapsulation of the packets for the MN. Consequently, this approach has disadvantages in terms of the accrual of packet loss and jitter by the redundant path and tunneling processing. The second approach is that the LMA controls the data traffic of the MN. The LMA knows the IP address of the pMAG or the nMAG during the handover of the MN and forwards the data traffic of the MN to the appropriate MAG for reduction of packet loss. In this approach, the data traffic of the MN is routed through the bi-directional tunnel between the LMA and the MAG, so that the delivery path is optimal. Consequently, we adopt the second approach, i.e., flow management by the LMA, as the method to control the data

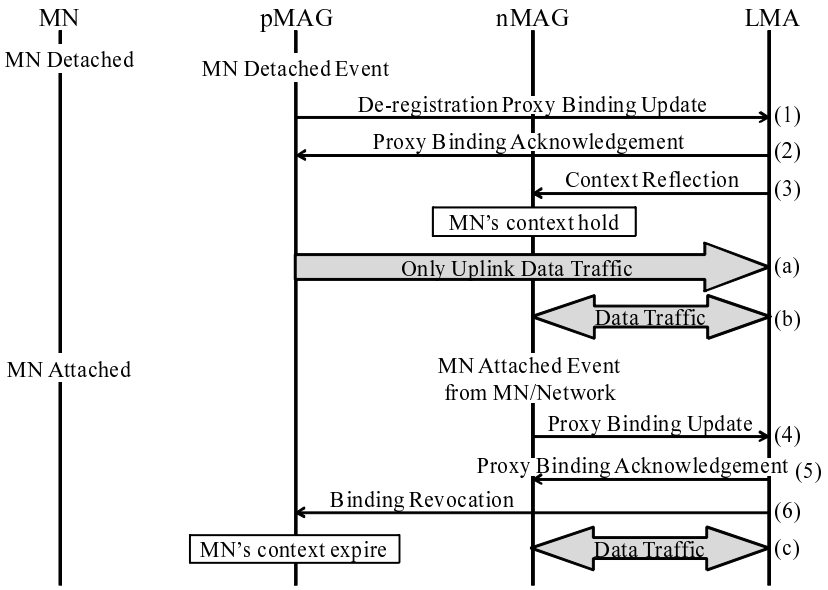

Figure 7: Signaling sequence of Context Reflector

traffic of the MN.

3.2 Overview of Context Reflector for Proxy Mobile IPv6

Since Context Reflector can carry any kinds of the context of the MN including the policy profile, the binding states, etc., it can optimize the handover sequence. It can be used as another fast handover mechanism for PMIPv6, too.

In Context Reflector, the LMA classifies the BCEs into the Proxy Binding Cache Entries (Proxy BCEs) and the Context Cache Entries (CCEs). The Proxy BCE is the BCE defined in PMIPv6 and contains the IP address of the MAG to which the MN currently attaches. The CCE is the BCE that is short lived with a lifetime and contains the context of the MN. The CCE in the LMA contains both pMAG's address and nMAG's address as the Proxy-CoA of the MN.

3.3 Signaling Operation

Figure 7 shows the signaling sequence of Context Reflector. Since certain security associations are already established between the LMA and the pMAG/nMAG for PMIPv6 operation, all the messages in Context Reflector are securely exchanged without establishment of a new security association.

As soon as the pMAG detects detachment of the MN, it sends the de-registration PBU to the LMA (Figure 7(1)). In the PBU, the pMAG sets the context flag and stores the context of the MN. The LMA verifies the message and removes the Proxy BCE for the MN. In addition, it creates a new CCE for the MN. The CCE lives until the LMA receives the PBU from the nMAG of the MN. Then the LMA sends the PBA to the pMAG in reply to the PBU (Figure 7(2)). After the LMA receives the de-registration PBU from the pMAG, it reflects the received context of the MN to the nMAG (Figure 7(3)). The LMA acquires the IP address of the nMAG from the context notified by the pMAG. This context transfer is done with a new message named the *Context Reflection* (CR). When the nMAG receives the CR, it stores the context of the MN and waits for the arrival of the MN. When the MN attaches to the nMAG, the nMAG sends the PBU (Figure 7(4)). The PBU overwrites the CCE with the new Proxy BCE in the

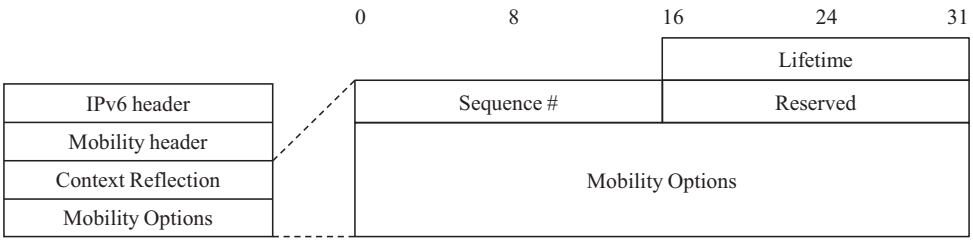

Figure 8: Format of the Context Reflection message

LMA. Then the LMA sends the PBA to the nMAG in reply to the PBU (Figure 7(5)). After processing the binding registration, the LMA sends the binding revocation message to the pMAG so that the pMAG can erase the context cache of the MN (Figure 7(6)). Since the context cache is managed with a lifetime, this revocation message is optional.

3.4 Flow Management

In Context Reflector, the LMA controls the data traffic of the MN to reduce packet loss for the MN during handover. As described in Section 2.2, the uplink data traffic of the MN, which is sent from the pMAG after the MN detaches from it, cannot be accepted by the LMA. However, in Context Reflector, the LMA still keeps the IP address of the pMAG as the Proxy-CoA of the MN in the CCE after receiving the de-registration PBU from the pMAG. The LMA can accept and route the delayed uplink data traffic of the MN delivered from the pMAG (Figure 7(a)). In addition, in Context Reflector, the LMA has already acquired the IP address of the nMAG and registered it as the Proxy-CoA of the MN before receiving the PBU sent by the nMAG. The LMA can accept the uplink data traffic of the MN sent before the operation by exchanging the PBU and the PBA is completed (Figure 7(b)). On the other hand, for the downlink data traffic of the MN, the LMA can either buffer the packets or send the packets to the nMAG (Figure 7(b)). When buffering the packets, the LMA sends them to the nMAG as soon as it receives the PBU from the nMAG. Since the pMAG notifies the IP address of the nMAG as the context of the MN to the LMA, the LMA can deliver the packets to the nMAG before the MN attaches to the nMAG. After the attachment of the MN and binding registration by the nMAG, all uplink/downlink data traffic of the MN is delivered through the nMAG (Figure 7(c)).

3.5 Message Formats

3.5.1 Context Reflection Message

We introduce *the Context Reflection (CR) message*, which is sent from the LMA to the nMAG to transfer the MN's context in secure unicast, e.g., in unicast with IPsec. Figure 8 shows the format of the Context Data option in the Mobility header. *The Lifetime field* contains the lifetime of the context of the MN. When the lifetime expires, the MN's context is removed even if the handover is in progress. *The Sequence Number field* contains the sequence number copied from that in the PBU message that transfers the MN's context.

3.5.2 Context Data Option

We introduce *the Context Data option* to store the MN's context in the De-Registration PBU message or the CR message. More than one Context Data options may be contained in a message. Figure 9 shows

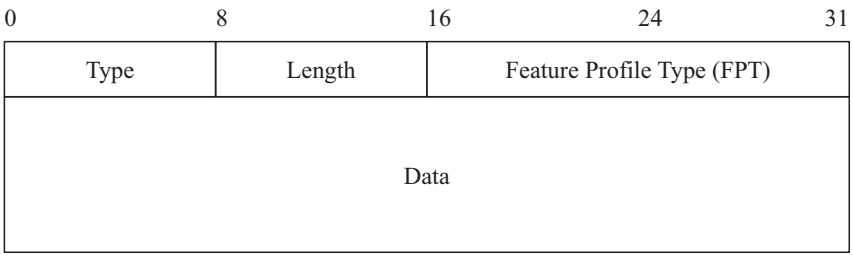

Figure 9: Format of context data option

the format of the Context Data option. *The Type field* is the option type and *the Length field* is the length of the option. *The Feature Profile Type (FTP) field* is the type of the data contained in *the Data field*.

3.6 nMAG discovery

Fast Handovers for Mobile IPv6 (FMIPv6)[8] is standardized for optimizing handover process of Mobile IPv6. When the MN discovers one or more new available access routers and predicts its handover, it sends the message to indicate its handover to the router to which the MN attaches currently. This message includes an IP address of the new access router to which the MN attaches after the handover. The router to which the MN attaches currently can acquire the IP address of the new access router by receiving the message from the MN. Therefore, FMIPv6 requires modifications to the MN for new access router discovery and detection of handover. However, modification to the MN is one of the reasons that the mobility protocols are not deployed. Since PMIPv6 is proposed as a solution of this problem, the MN should not be modified in the extension protocol to PMIPv6. Consequently, in Context Reflector, the pMAG predicts the handover of the MN and discover the nMAG instead of the MN, and it is assumed that the pMAG can acquire the IP address of the nMAG in some way.

4 Related Work and Comparison

This section compares in detail Context Reflector with other extension protocols to PMIPv6; Fast Handovers for PMIPv6[9] and A Fast Handover Scheme in Proxy Mobile IPv6[10].

4.1 Fast Handovers for PMIPv6

In Fast Handovers for PMIPv6 (hereafter called “FPMIPv6”), the context of the MN such as the MN-ID and the MN-HNP is sent from the pMAG to the nMAG directly. Therefore, a bi-directional tunnel between the two MAGs is established and all data traffic of the MN is delivered through this bi-directional tunnel.

Figure 10 shows the handover procedure in FPMIPv6. The MN detects that a handover is imminent and reports the information of the MN such as the MN-ID and the IP address of the nMAG. Then, the access network to which the MN currently attaches signals HO Initiate to the pMAG that indicates the handover of the MN (Figure 10(1)). When the pMAG detects the handover of the MN, the Handover Initiate (HI) message and the Handover Acknowledge (HAck) message are exchanged between the pMAG and the nMAG in order to transfer the context of the MN and establish a new bi-directional tunnel between them (Figure 10(2)). Then, the MN moves and switches its attachment point from the pMAG to the nMAG (Figure 10(3), (4)). After the MN attaches to the nMAG, the two MAGs may exchange the HI and the HAck to complete the packet forwarding (Figure 10(5)). Finally, the PBU and the PBA are exchanged between the nMAG and the LMA to update the binding of the MN in the LMA (Figure10(6)).

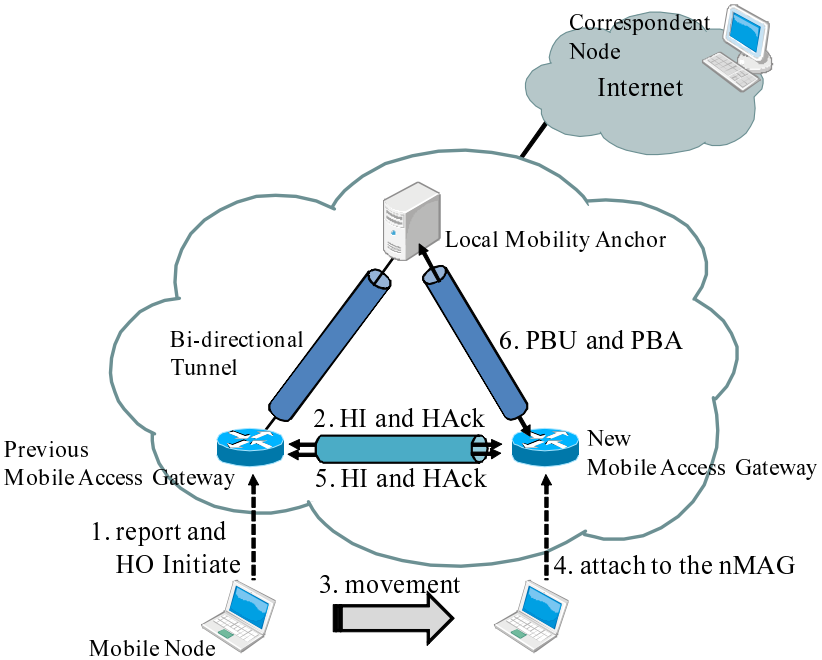

Figure 10: Handover procedure in FPMIPv6

After establishment of the bi-directional tunnel, the data traffic of the MN is forwarded by the pMAG and the nMAG. The downlink data traffic of the MN is forwarded from the pMAG to the nMAG and the nMAG buffers them until the attachment of the MN. The nMAG starts forwarding the buffered downlink data traffic of the MN as soon as the MN attaches to it. Similarly, the uplink data traffic of the MN is forwarded from the nMAG to the pMAG through the bi-directional tunnel. Therefore, all data traffic of the MN is delivered from/to the LMA to/from the nMAG via the pMAG. After the operation by exchanging the PBU and the PBA, the data traffic of the MN from/to the LMA to/from the nMAG directly because the LMA updates the Proxy-CoA of the MN to the IP address of the nMAG.

4.2 A Fast Handover Scheme in Proxy Mobile IPv6

A Fast Handover Scheme in Proxy Mobile IPv6 (hereafter called “Fast Handover Scheme”) uses bi-directional tunnels between the LMA and the pMAG/nMAG. Before the MN attaches to the nMAG, the LMA can acquire the IP address of the nMAG and updates the Proxy-CoA of the MN in the BCE.

Figure 11 shows the handover procedure for Fast Handover Scheme. At the beginning, the link-specific pre-handover procedure happens and the access network to which the MN currently attaches signals HO Initiate to the pMAG that indicates the handover of the MN (Figure 11(1)). When the pMAG detects the handover of the MN, it sends the Fast PBU that includes the MN-ID and the IP address of the nMAG, and the LMA returns the Fast PBA (Figure 11(2)). Subsequently, the LMA sends the Reverse PBU including the context of the MN such as the MN-ID and the MN-HNP to the nMAG. By the Reverse PBU, the nMAG can acquire the context of the MN before the MN attaches to the nMAG. The nMAG returns the Reverse PBA to the LMA and waits for the arrival of the MN (Figure 11(3)). Then, the LMA updates the Proxy-CoA of the MN to the IP address of the nMAG acquired from the Fast PBU, so that delivery of all data traffic of the MN starts via the nMAG. Additionally, the downlink data traffic of the MN is buffered in the nMAG until the MN attaches to the nMAG.

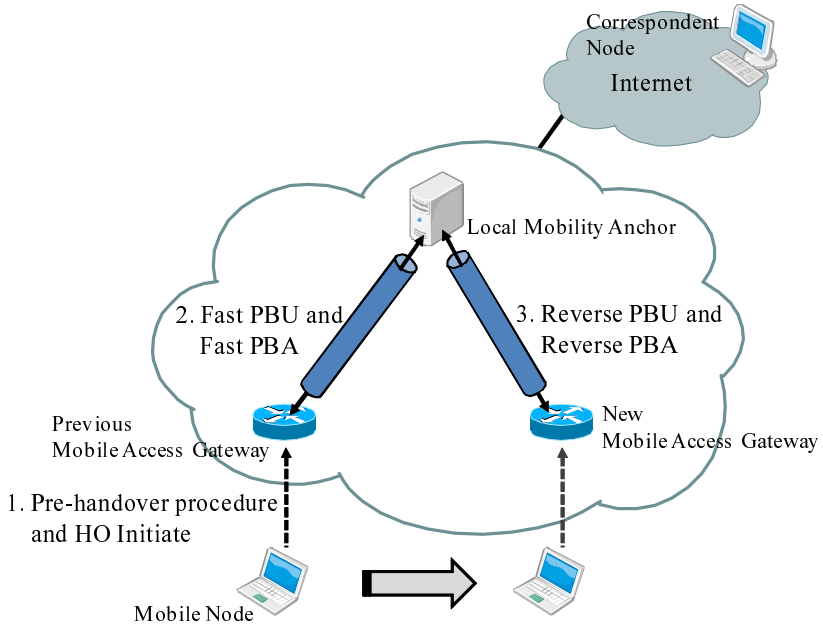

Figure 11: Handover procedure of Fast Handover Scheme

Table 1: Comparison of the three extension protocols to PMIPv6

	Context Reflector	FPMIPv6	Fast Handover Scheme
Security association	LMA-pMAG/ nMAG	pMAG-nMAG	LMA-pMAG/ nMAG
Entity performing flow management	LMA LMA	pMAG and nMAG	LMA and nMAG
Candidate traffic of flow management	uplink and downlink	uplink and downlink	downlink
Delivery path of the data traffic of the MN during handover	optimal	redundant	optimal
Optimizing handover process	packet loss and handover latency	packet loss and handover latency	packet loss
Entity requiring the extension	LMA, pMAG and nMAG	pMAG and nMAG	LMA, pMAG and nMAG

4.3 Comparison

Table 1 shows the comparison of three extension protocols to PMIPv6.

4.3.1 Security Association

A security association is used for transferring the context of the MN securely. In Context Reflector and Fast Handover Scheme, the existing security association between the LMA and the pMAG/nMAG is used because the context of the MN is transferred from the pMAG to the nMAG via the LMA (the second approach described in Section 3.1.1). Therefore, it is not required to establish a new security association.

However, in FPMIPv6, since the context of the MN is transferred from the pMAG to the nMAG directly (the first approach described in Section 3.1.1), each MAG must establish new security associations to the other MAGs and the overhead of establishment of the new security associations occurs.

4.3.2 Flow Management

In these protocols, the data traffic of the MN is controlled by some mobility entities in the network in order to reduce packet loss during handover. In Context Reflector, only the LMA controls the data traffic of the MN. Since the LMA keeps both pMAG's address and nMAG's address in the CCE in the LMA, it can accept the uplink data traffic of the MN from both the pMAG and the nMAG. Therefore, packet loss of the uplink data traffic of the MN during handover can be prevented. Since the LMA can acquire the IP address of the nMAG before the MN attaches to the nMAG, the downlink data traffic of the MN is forwarded to the nMAG or buffered by the LMA. Therefore, packet loss of the downlink data traffic of the MN does not occur, too. In Fast Handover Scheme, the LMA and the nMAG control the data traffic of the MN. After the LMA receives the Fast PBU including the MN-ID and the IP address of the nMAG from the pMAG, it forwards the downlink data traffic of the MN to the nMAG and the nMAG buffers it. Therefore, packet loss of the downlink data traffic of the MN does not occur. The LMA updates the Proxy-CoA of the MN to the address of the nMAG upon receiving the Fast PBU. Then it cannot accept the delayed uplink data traffic of the MN delivered from the pMAG because the source IP address does not match the registered Proxy-CoA on the BCE of the MN. Therefore, packet loss of the uplink data traffic of the MN occurs. In Context Reflector and Fast Handover Scheme, since the LMA controls the data traffic of the MN (the second approach described in Section 3.1.2), the delivery path of the data traffic of the MN is optimal. On the other hand, the data traffic of the MN is controlled by the pMAG and the nMAG in FPMIPv6 (the first approach described in Section 3.1.2). Since the LMA keeps the IP address of the pMAG as the Proxy-CoA of the MN during handover and all uplink data traffic of the MN is sent from the pMAG to the LMA, packet loss of the uplink data traffic of the MN does not occur. In addition, packet loss of the downlink data traffic of the MN also does not occur because the downlink traffic of the MN is forwarded from the pMAG to the nMAG and buffered by the nMAG. However, since the delivery path of the data traffic of the MN is redundant and tunneling processing must be needed, FPMIPv6 has the large overhead of processing flow management. Consequently, in these three protocols, Context Reflector is the only protocol that can prevent packet loss of the uplink/downlink data traffic of the MN and forward the data traffic of the MN by the optimal path.

In Context Reflector, only the LMA controls the data traffic of the MN. If the number of MNs doing handover becomes large, the LMA may become the bottleneck. There can be multiple LMAs in a PMIPv6-Domain. Therefore, this problem can be solved by distributing the process of the handover of the MN multiple LMAs.

4.3.3 Optimizing handover process

The context of the MN, that is treated in Fast Handover Scheme, contains only the policy profile and the Proxy-CoA of the MN. However, Context Reflector and FPMIPv6 propose transfer of the context of the MN such as states of AAA, ROHC, QoS, etc. These protocols are able to reduce handover latency because the services, such as AAA, ROHC and QoS, are able to be re-established quickly after handover. Consequently, Context Reflector and FPMIPv6 can reduce not only packet loss but also handover latency.

4.3.4 Entity requiring the extension

In FPMIPv6, it is not necessary to extend the LMA. It is because this protocol transfers the context of the MN and forwards the data traffic of the MN between the two MAGs directly not via the LMA. However,

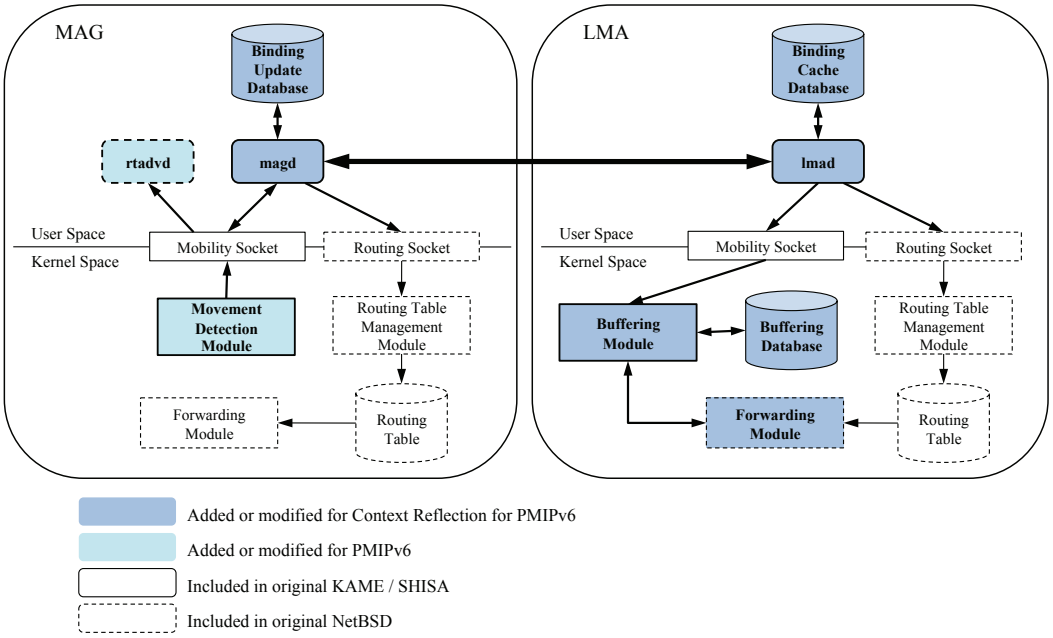

Figure 12: Diagram of context transfer for PMIPv6 implementation

in Context Reflector and Fast Handover Scheme, it is necessary to extend the LMA, the pMAG and the nMAG. Therefore, these two protocols have more modification cost than FPMIPv6.

5 Implementation and Evaluation

5.1 Implementation of Context Reflector for PMIPv6

We first implemented PMIPv6 on NetBSD 4.99.52 by modifying the SHISA/KAME stack[11, 12], which is an open source of MIPv6 on BSD Unix systems, and then extended this implementaiton to support the context reflection. Figure 12 shows the diagram of our implementation. We added two daemon programs to the SHISA/KAME stack: *lmad* on the LMA and *magd* on the MAG. The *lmad* maintains the MN's information and executes signaling with the MAG. The *lmad* opens the Routing Socket to change the routing to the MN by modifying the routing table in the kernel space. The *magd* maintains the MN's information and executes the signaling with the LMA. We modified a daemon *rtadvd*, which periodically sends the Router Advertisement message. We also added *the movement detection module*, *the buffering module* and *the buffering table* in the kernel space. *The Mobility Socket (MIPSOCK)*, which was introduced in the KAME/SHISA stack, was used for the communication among the movement detection module, *lmad*, and *magd*.

5.2 Processing Time at Handover and the Packet Loss Period

We measured the processing time at handover in PMIPv6 and Context Reflectior for PMIPv6 in our test network. Our test network consists of a LMA, two MAGs, a MN, a CN, and a router. The router is supposed as the Internet. The LMA and the CN are connected to the router. IEEE802.11g is used for the wireless link between the MN and the MAGs. On the MAGs, *dummynet* is installed so as to vary the delay between the MAGs and the LMA.

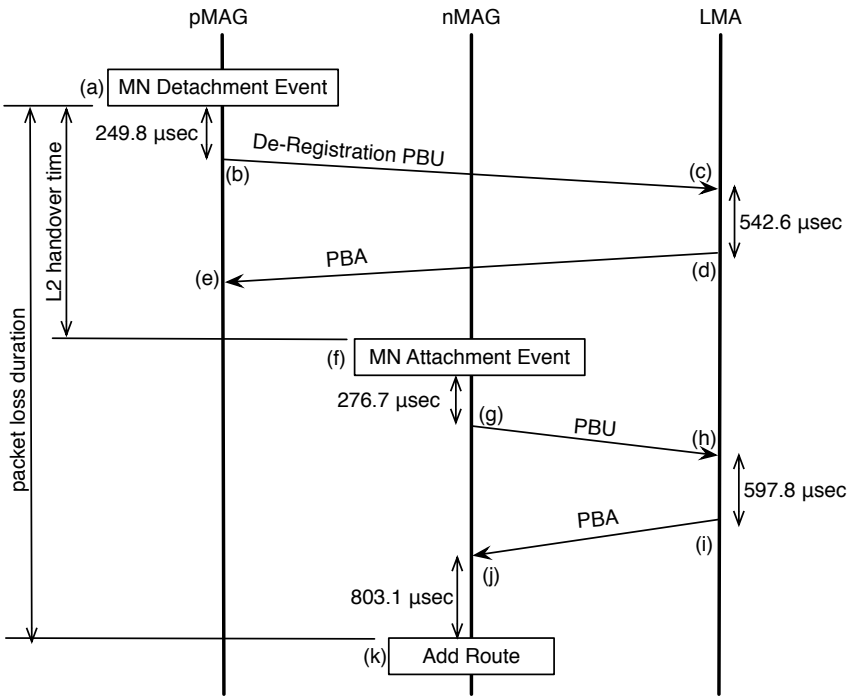

Figure 13: Handover processing time in PMIPv6

Figure 13 shows the processing time at a handover in PMIPv6. We used the free-run counter of the CPU. The value of the free-run counter is incremented by 1 every CPU clock. Each value in the figure is the average of measured values in 20 times. As shown in the figure, we assume that the L2 handover time ((a)∼(f)) is longer than the period from the time when the pMAG detects the MN's detachment event to the time when the pMAG receives the PBA ((a)∼(e)) because the L2 handover time usually requires more than 10 ms. The time required for a handover in PMIPv6 is the period between (a) and (k). In this period, packets are dropped. As a result, the time required for a handover and the period in which packets are dropped in PMIPv6 can be expressed as follows:

$$L2\_handover\_time + ((e) \sim (f)) + ((g) \sim (h)) + ((i) \sim (j)) + RTT_{nMAG-LMA} =$$
$$L2\_handover\_time + 276.7(\mu sec) + 597.8(\mu sec) + 803.1(\mu sec) + RTT_{nMAG-LMA} =$$
$$L2\_handover\_time + RTT_{nMAG-LMA} + 1677.6(\mu sec)$$

Figure 14 shows the processing time at a handover in Context Reflectior for PMIPv6 in case that the size of the context is 64 bytes. Each value in the figure is the average of measured values in 20 times. We assume that the L2 handover time ((a)∼(g)) is longer than the period from the time when the pMAG detects the MN's detachment event to the time when the nMAG receives and stores the MN's context ((a)∼(f)). In Context Reflectior for PMIPv6, the period in which packets are dropped is equal to the L2 handover time.

6 Conclusion

This paper proposed a simple context transfer mechanism named Context Reflectior for Proxy Mobile IPv6 and compared it with other extension protocols to PMIPv6.

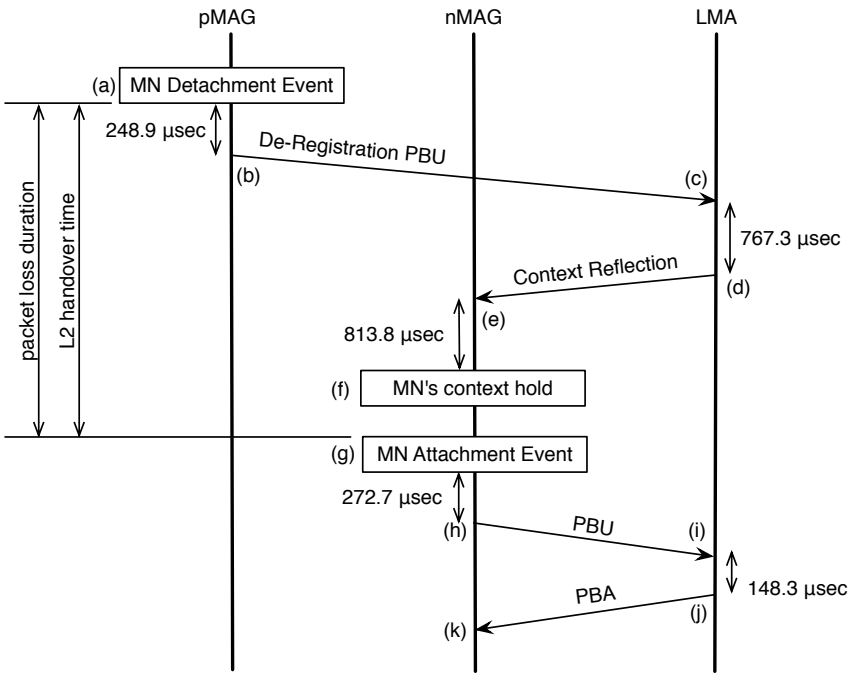

Figure 14: Handover processing time in Context Reflectior for PMIPv6

In Context Reflection, by transferring the context of the MN, handover latency can be reduced. Additionally, by holding both pMAG's address and nMAG's address as the Proxy-CoA of the MN in the CCE and controlling the data traffic of the MN by the LMA, packet loss of the data traffic of the MN can be prevented. Processing overhead is small because of use of the existing security association and the optimal delivery path of the data traffic of the MN.

Consequently, we can make a conclusion that Context Reflectior for Proxy Mobile IPv6 is a useful protocol for optimizing handover process of PMIPv6.

References

[1] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, *IETF*, Jun. 2004.

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdfury, and B. Patil. Proxy Mobile IPv6. RFC5213, *IETF*, Jun. 2008.

[3] K. S. Kong, W. J. Lee, Y. H. Han, M. K. Shin, and H. R. You. Mobility management for all-ip mobile networks: Mobile ipv6 vs. proxy mobile ipv6. *IEEE Wireless Communications*, April 2008.

[4] K. S. Kong, W. J. Lee, and Y. H. Han. Handover latency analysis of a network-based localized mobility management protocol. In *Proc. of IEEE ICC 2008*, 2008.

[5] S. Kiriyama, R. Wakikawa, J. Xia, and F. Teraoka. Context Reflector for Proxy Mobile IPv6. In *Proceedings of The 3rd Internatinal Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2009)*, March 2009.

[6] J. Kempf. Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network. RFC3374, *IETF*, Sep. 2002.

[7] M. Liebsch, A. Muhanna, and O. Blume. Transient Binding for Proxy Mobile IPv6. Internet Draft, *IETF*, Jul. 2008. work in progress.

[8] R. Koodli. Mobile IPv6 Fast Handovers. RFC 5268, *IETF*, Jun. 2008.

[9] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia. Fast Handovers for PMIPv6. Internet Draft, *IETF*, Jul. 2008. work in progress.

[10] Y. Han and B. Park. A Fast Handover Scheme in Proxy Mobile IPv6. Internet Draft, *IETF*, Jul. 2008. work in progress.

[11] SHISA, . http://www.mobileip.jp/.

[12] The KAME project, . http://www.kame.net/.

Sawako Kiriyama received her bachelor degree in Information and Computer Science from Keio University, Japan in 2007 and master degree in Open Environment System from Graduate School of Keio University, Japan in 2009. Her interests in research include mobile computing, Internet protocols IPv6, mobile IPv6, proxy mobile IPv6, system operations, BSD operating systems.

Ryuji Wakikawa received his Ph.D. degree in Media and Governance from Keio University in 2009 and M.E. degree in Media and Governance from Keio University in 2001. He was an Assistant Professor, Faculty of Environment Information, Keio University. He is now a senior researcher at Toyota InfoTechnology Center Co., Ltd. He has participated in IETF since 49th meeting and contributed to MIP6, NEMO, Monami6, MEXT, AUTOCONF, MANET working groups while publishing several RFCs and internet drafts. He has served or is currently serving on the organizing or program committees of international conferences and workshops such as ACM MobiArch, ACM SIGCOMM, MobiWorld, WONEMO and so forth. His research interests are Mobile Computing, Mobile IP, Mobile Ad-hoc Network, and Mobile Network. He is a member of ACM and WIDE.

Fumio Teraoka received a master degree in electrical engineering and a Ph.D. in computer science from Keio University in 1984 and 1993, respectively. He joined Canon Inc. in 1984 and then moved to Sony Computer Science Labs., Inc. (Sony CSL) in 1988. Since April 2001, he is a professor of Faculty of Science and Technology, Keio University. He received the Takahashi Award of JSSST (Japan Society for Software Science and Technology) and the Motooka Award in 1991 and 1993, respectively. He also received the Best Paper Award in 2000 from IPSJ (Information Processing Society Japan). His research interest covers computer network, operating system, and distributed system. He contributed to the activity of the Mobile working group of IETF by developing Virtual IP (VIP). He was a board member of the WIDE Project from 1991 to 2010. He was a board member of IPSJ from 2000 to 2002. He was a board member of JSSST from 2005 to 2009. He is a member of ACM, IEEE, JSSST, IPSJ, and IEICE.