An Optimized Scheme for Mobile IPv6 Handover between Domains Based on AAA*

Seonggeun Ryu and Youngsong Mun

School of Computing, Soongsil University,
Sangdo 5 Dong Dongjak Gu, Seoul, Korea
sgryu@sunny.ssu.ac.kr, mun@computing.ssu.ac.kr

Abstract. When Mobile IPv6 is deployed in commercial network, a mobile node needs AAA services for authentication, authorization and accounting. AAA and Mobile IPv6 are operated independently. Hence schemes which merge these protocols have been emerged. These schemes enable the mobile node to establish a security association between the mobile node and a home agent, and to perform a home binding update during AAA authentication procedure. But these schemes introduce lots of signal messages and long handover latency during the handover, since Route Optimization mode for Mobile IPv6 is performed using Return Routability procedure. To solve this problem, we propose an optimized scheme which performs Route Optimization mode via the AAA infrastructure between the home agent and a correspondent node instead of Return Routability procedure. For performance evaluation, we analyze handover latency in three scenarios. We then show that the proposed scheme reduces handover latency like the average of 58% compared with the existing scheme.

1 Introduction

As mobile devices like laptops and PDAs are improved and wireless/mobile communications and networking were propagated widely, mobile users for Internet access have increased. Hence mobility support between administrative domains is required, since these users want to use a high-quality Internet service at any administrative domain.

Mobile IPv6 [1] which supports mobility of a mobile node (MN) in IPv6 networks has been standardized by Internet Engineering Task Forces (IETF). When Mobile IPv6 is deployed in commercial network, the MN needs AAA services for authentication, authorization and accounting. AAA and Mobile IPv6 are operated independently. Hence schemes which merge these protocols have been emerged. Frank Le's scheme [2] among these schemes can support a fast handover, since it enables the MN to establish a security association between

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(IITA-2005-C1090-0502-0009)

the MN and its home agent (HA), and to perform a home binding update during AAA authentication procedure. However, this scheme introduces lots of signal messages and long handover latency during the handover, because Route Optimization mode for Mobile IPv6 is performed by using Return Routability procedure. Return Routability procedure consists of Home of Test Init (HoTI) / Home of Test (HoT) and Care-of Test Init (CoTI) / Care-of Test (CoT) messages which cause long handover latency.

To solve this problem, we propose an optimized scheme for Route Optimization mode by using the AAA infrastructure between the HA and a correspondent node (CN) instead of Return Routability procedure. When the MN performs AAA procedure, it embeds a home Binding Update (BU) message and the CN's information (address and the Network Access Identifier (NAI) [3]) in a request message of AAA procedure. The BU message and the CN's information are delivered to the HA through AAA procedure. After the HA performs the home binding update, it creates a BU message to the CN for Route Optimization mode. The HA then sends the BU message to the CN via the AAA infrastructure between itself and the CN.

The proposed scheme can reduce signal messages and handover latency during the handover, because Return Routability procedure for Route Optimization mode is not performed. The proposed scheme also can get a security benefit, since it uses the AAA infrastructure which is secured by IPsec [6] and TLS [7].

The rest of this paper is organized as follows: in section 2, basic protocols and Frank Le's scheme are presented as related works. The proposed scheme is described in section 3, and in section 4 the proposed scheme is evaluated through analysis of handover latency. Finally, in section 5 we conclude discussion with future study.

2 Related Works

Mobile IPv6 protocol enables an MN to keep connections to an HA and a CN, although the MN changes a point of attachment to network. In Mobile IPv6 the MN has two addresses of a home address (HoA) and a care-of address (CoA). The HoA is generated in a home network, which never be changed although the MN moves into another network, and hence the HA and the CN identify the MN as the HoA. The CoA is generated in a visited network whenever it moves, and represents a current location. Mobile IPv6 protocol binds the CoA to the HoA. In Mobile IPv6 the MN uses Route Optimization mode consisting of Return Routability procedure and a binding update to the CN to communicate with the CN directly. Return Routability procedure consists of HoTI/HoT and CoTI/CoT message, and it generates a key between the MN and the CN, and then a BU message to the CN is authenticated by the generated key. Whenever the MN moves between networks, a process for mobility support is required and is called a handover. The handover consists of a movement detection, an address configuration, a home binding update, Return Routability procedure,

and a binding update to the CN. The MN cannot communicate with the CN during the handover.

When Mobile IPv6 is deployed in commercial networks, the MN needs AAA [4] services to allow it to access to any service provided by an administrative domain different from its home domain. AAA supports authentication and authorization for the MN and collects MN's accounting information [5]. AAA is a distributed security model which consists of distributed clients and central servers. In AAA, all of connections between entities are secured by IPsec and additionally by TLS.

When the MN moves into a foreign domain, it needs authorization to attach to the foreign domain. Hence AAA is required to enable the MN to get access to the foreign domain. After getting the access permission to the foreign domain through AAA, Mobile IPv6 is performed to support mobility. These two protocols are performed in order, so signal messages and handover latency are increased. Schemes which merge two protocols have studied to solve these problems. This paper is based on Frank Le's scheme among these schemes.

In Frank Le's draft, he specifies a new application to Diameter [8] that enables Mobile IPv6 to roam between administrative domains, and provides a solution for Mobile IPv6 and AAA interworking. Besides supporting authentication and authorization for the MN, the AAA infrastructure can also be used for distributing the security association which is necessary to support mobility. Optionally, the AAA infrastructure can be used to optimize authentication, authorization and mobility in a common procedure. In this paper, we focus on the optimization scheme in Frank Le's draft.

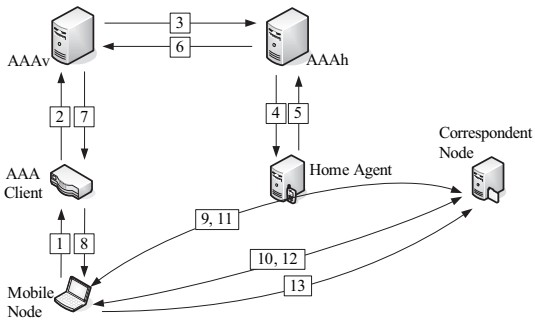

Fig. 1. Message flows of Frank Le's scheme

Figure 1 shows message flows of Frank Le's scheme, and the numbers in Fig. 1 are the order of flows. When entering a foreign administrative domain, the MN

receives router advertisements and it retrieves the local challenge, the visited network identifier and the information to derive a CoA. The MN computes the CoA and creates the request message with the CoA as the source IP address, the AAA Client address as the destination IP address, the NAI, the long-term security key shared with its AAAh, and other parameters. The MN creates the BU message, which will be embedded in the request message. The BU message will be forwarded to the designated HA via the AAA infrastructure. The MN then sends the request message to the AAA Client. Frank Le's draft does not define how the authentication information is exchanged between the MN and the AAA Client. This may be performed using the protocol defined by the PANA working group in IETF.

When the AAA Client receives the request message, it converts this message to the AA Registration Request (ARR) message. The ARR message includes the MN's NAI, MIP-Home-Binding-Update AVP containing the BU message and other AVPs. The AAA Client sends the ARR message to the AAA home server (AAAh) via the AAA visited server (AAAv). When receiving the ARR message from the AAAv, the AAAh verifies the message coming from a valid AAAv. The AAAh then authenticates the user using the NAI provided by the MN. The AAAh forwards the MIP-Home-Binding-Update AVP to the HA in the HA MIPv6 Request (HOR) message. If the MN asks for some security keys, the AAAh performs the appropriate steps and eventually sends the corresponding messages in order to achieve the key distribution.

Upon receipt of the HOR message, the HA verifies the message. It processes the MIP-Home-Binding-Update AVP, updates the Binding Cache Entry (BCE), and then creates the Binding Acknowledgement (BA) message. If the MN requests key distribution, the HA computes the key for the security association with the MN from the received data. The HA creates the HA MIPv6 Answer (HOA) message including the MIP-Binding-Acknowledgement AVP containing the BA message, and it then send the HOA message to the AAAh.

After receiving the HOA message, the AAAh verifies the message. The AAAh then creates the AA Registration Answer (ARA) message including MIP-Binding-Acknowledgement AVP and other AVPs, and sends the message to the AAA Client via the AAAv. When receiving the ARA message from the AAAv, the AAA Client converts the message to a reply message and sends the reply message to the MN.

When receiving the reply message from the AAA Client, the MN authenticates the network according to the network authentication data sent by the AAA Client. If the MN requested the key distribution, it creates the security associations from the received keying material. The MN then processes the BA message, and it performs Return Routability procedure, which the HoTI/HoT and CoTI/CoT messages are exchanged between the MN and the CN. The MN then creates a BU message and sends the BU message to the CN. When receiving the BU message from the MN, the CN updates the BCE for the MN. Finally, the handover is completed and the MN and the CN can communicate directly.

3 The Proposed Scheme

Frank Le's scheme can optimize a handover, since the AAA infrastructure can be used to support mobility procedures and to optimize authentication, authorization and mobility in a common procedure. However, Frank Le's scheme must perform Return Routability procedure for Route Optimization mode. Therefore, handover latency is long because of messages used in Return Routability procedure.

To solve this problem, we propose an optimized scheme for Route Optimization mode by using the AAA infrastructure between the HA and a CN instead of Return Routability procedure. When the MN requests AAA authentication, it embeds a home BU message and the CN's information (address and NAI) in a request message of AAA procedure. When the HA receives the BU message and CN's information via the AAA infrastructure, it performs the home binding update and creates a BU message to the CN. The HA then sends the BU message to the CN via the AAA infrastructure between itself and the CN.

For the proposed scheme, we assume the followings. The proposed scheme is based on Frank Le's scheme, and the CN must be supported by AAA. When the MN sends the request message to an AAA Client, the CN's address and NAI must be able to be embedded in the message. The MN must have known the CN's NAI using an appropriate manner in advance. The CN's address and NAI will be forwarded from the MN to the HA via the AAA infrastructure. The HA must be able to create an AAA message like as the ARR message, and then an MIP-CN-Binding-Update AVP containing a BU message for the CN must be included in the created message. We define the MIP-CN-Binding-Update AVP like as the MIP-Home-Binding-Update AVP in Frank Le's scheme. The CN must be able to process the MIP-CN-Binding-Update AVP.

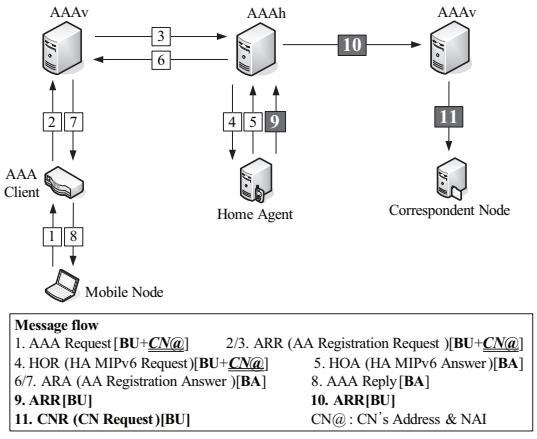

Fig. 2. Message flows of the proposed scheme

Figure 2 shows message flows of the proposed scheme, and the numbers in Fig. 2 are the order of flows. In the proposed scheme the processes from the number 1 to the number 8 in Fig. 2 are the same as Frank Le's scheme except the case that the CN's address and NAI are included in the AAA request.

When receiving the HOR message from AAAh, the HA processes MIP-Home-Binding-Update AVP and creates a BA message. The HA then creates a BU message for the CN with the MN's CoA as the source IP address, the CN's address as the destination IP address, and the MN's HoA as the home address option. The BU message is converted into a MIP-CN-Binding-Update AVP. The HA then sends the ARR message including the MIP-CN-Binding-Update AVP to CN's NAI. Upon receipt of the ARR message, the CN processes the MIP-CN-Binding-Update AVP, and then BCE for the MN is updated. Finally, Route Optimization mode is completed and the MN and the CN can communicate directly.

The proposed scheme does not need Return Routability procedure for Route Optimization mode, because the mode is completed via the AAA infrastructure. Therefore, the proposed scheme can reduce signal messages and handover latency.

4 Performance Evaluations

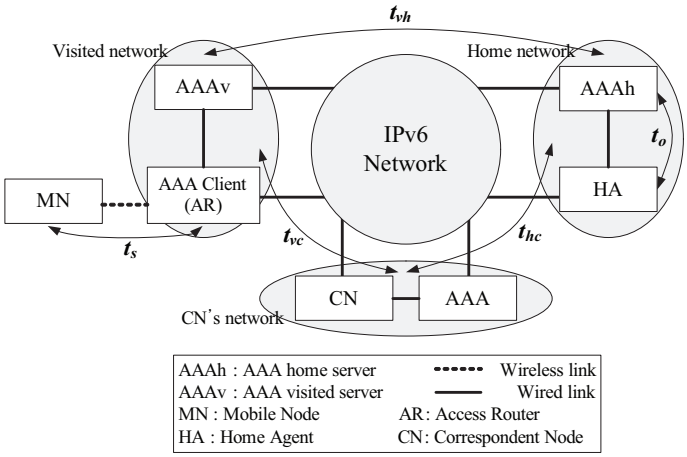

Fig. 3. A simple model for analysis

In this section we make an analytic comparison of Frank Le's scheme with the proposed scheme in terms of handover latency. The handover latency consists of link layer establishment delay and signaling delay. We focus on signaling delay, since protocols of link layer are various. Hence, we define a period of handover

latency as one from a moment of the movement detection to a moment of Route Optimization mode. For simplicity we consider the model illustrated in Fig. 3 referring to [9].

The notations in Fig. 3 are used as the followings, referring to [9], [10]. The delay between the MN and the AAA Client is t_s, which is the time to send a message over the subnet via wireless link. Also, the delay between entities in a same network is t_o , which is the time to send a message over one hop via wired link. The delay between the entities in the visited network and the entities in the home network is t_{vh}, the delay between the entities in the home network and the entities in the CN's network is t_{hc}, and the delay between the entities in the visited network and the entities in the CN's network is t_{vc}. In this paper we only consider the scenario where the CN is in its home network, although the CN is a mobile node. In general, we assume that the processing and queuing times are negligible, since these times are much shorter than above times [10].

4.1 Analysis of Frank Le's Scheme

We analyze Frank Le's scheme referring to Fig. 1. In Frank Le's scheme AAA procedure and mobility support are performed in a common procedure. Therefore, the time for the AAA authentication and mobility support is given by

$$T_{Le-AAA-BU} = 4t_s + 4t_o + 2t_{vh}. \tag{1}$$

$T_{Le-AAA-BU}$ is a transmission time consisting of transmission times for Router Solicitation(RS)/Router Advertisement(RA) messages and messages from the number 1 to the number 8 in Fig. 1.

After the home binding, the MN performs Return Routability procedure for Route Optimization mode. In the procedure HoTI/HoT and CoTI/CoT messages are exchanged between the MN and the CN referring to Fig. 1. The MN then creates a BU message and sends the message to the CN. Therefore, Route Optimization mode is completed and the time for this procedure is given by

$$T_{Le-RO} = 5t_s + 2t_{vh} + 2t_{hc} + 2t_{vc}. \tag{2}$$

When Route Optimization mode is completed, the handover is completed. Therefore, handover latency is the sum of Eq. 1 and 2, and is equal to

$$T_{Le} = 9t_s + 4t_o + 4t_{vh} + 2t_{hc} + 2t_{vc}. \tag{3}$$

4.2 Analysis of the Proposed Scheme

Since the proposed scheme is based on Frank Le's scheme, the AAA authentication and mobility support are the same as Frank Le's scheme ($T_{Le-AAA-BU} = T_{prop.-AAA-BU}$). Analysis of the proposed scheme refers to Fig. 2. In the proposed scheme the HA creates a BU message and send the message to the CN

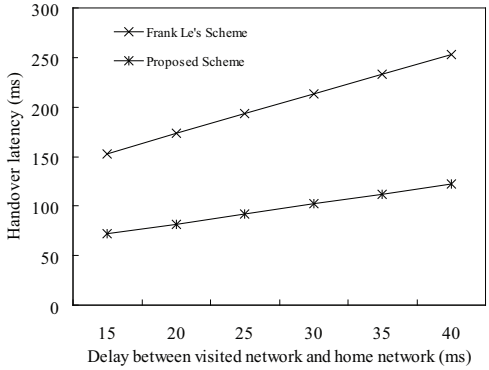

Fig. 4. Handover latency vs. delay between the MN and its home network

via the AAA infrastructure between the HA and the CN. Therefore, the times for Route Optimization mode and handover latency are equal to

$$T_{prop.-RO} = 2t_o + t_{hc}, \tag{4}$$

$$T_{prop.} = 4t_s + 6t_o + 2t_{vh} + t_{hc}. \tag{5}$$

4.3 Numerical Results

In this section we present some results based on the previous analysis. We assume $t_s = 10ms$ and $t_o = 2ms$ as in [9], considering relatively low bandwidth in the wireless link. Handover latencies for two schemes are calculated by Eq. 3 and 5 in three scenarios, respectively.

Impact of the delay between the MN and its home network We set $t_{vc} = 5ms$ and $t_{hc} = 10ms$, since we assume in this scenario that the distance between the visited network and the CN's network is close. Figure 4 shows handover latencies according to t_{vh}, and it shows that the proposed scheme reduces handover latency in comparison with Frank Le's scheme.

Impact of the delay between the MN and the CN We set $t_{vh} = 0$ and $t_{vc} = t_{hc}$, since we assume in this scenario that the MN is in its home network. In Fig. 5 handover latencies of the proposed scheme hardly increase according to t_{vc}, since Route Optimization mode for the proposed scheme does not use networks between the MN and the CN.

Impact of the wireless link delay We set $t_{vh} = t_{hc} = t_{vc} = 10ms$, since we assume in this scenario that network topologies are fixed. The wireless link delay

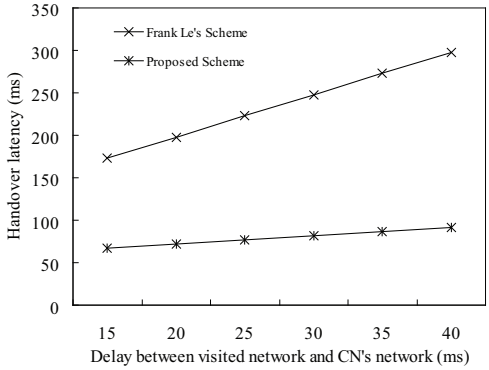

Fig. 5. Handover latency vs. delay between the MN and the CN

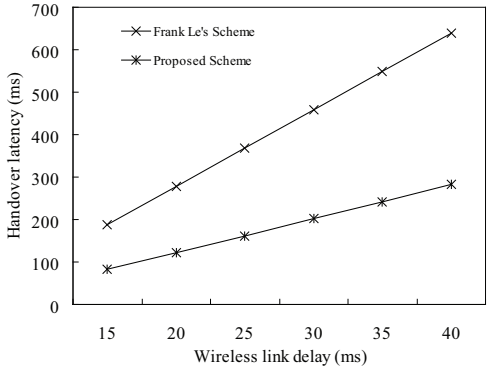

Fig. 6. Handover latency vs. wireless link delay

has an influence on handover latency. Especially, in Fig. 6 Frank Le's scheme is influenced considerably by the wireless link delay, since in Frank Le's scheme the MN sends and receives many messages via the wireless link in comparison with the proposed scheme.

5 Conclusions and Future Study

Mobile IPv6 does not provide any specific support for mobility passing through different administrative domains, which limits the applicability of Mobile IPv6 in a large scale commercial deployment. For Mobile IPv6 to be deployed in commercial networks, there therefore has to be AAA support for the protocol. Frank Le's scheme provides a solution for Mobile IPv6 and AAA interworking. It also can support a fast handover, since it enables an MN to establish a security association between the MN and an HA, and to perform a home binding

update through AAA procedure. However, Frank Le's scheme introduces a lot of signal messages and long handover latency during the handover, since Route Optimization mode is performed using Return Routability procedure.

To solve this problem, we propose an optimized scheme for Route Optimization mode that the HA performs the binding update for a CN by using the AAA infrastructure between the HA and the CN instead of Return Routability procedure. The proposed scheme can reduce handover latency during the handover, because Return Routability procedure for Route Optimization mode is not performed. The proposed scheme also can get a security benefit, since it uses the AAA infrastructure which is secured by IPsec and TLS. We have shown that the proposed scheme reduces handover latency like the average of 58% by comparison with Frank Le's scheme.

Fast Handovers for Mobile IPv6 (FMIPv6) [11] and Hierarchical MIPv6 (H MIPv6) [12] have been standardized in IETF. FMIPv6 is a enhanced handover scheme for Mobile IPv6, as portions of layer 3 handover are peformed layer 2 handover. HMIPv6 reduces location updates, since mobility is managed locally. Therefore, the proposed scheme can be considered to be used in FMIPv6 or HMIPv6, since these mechanisms have enhanced Mobile IPv6.

References

1. Johnson, D., Perkins, C., and Arkko J.: Mobility Support in IPv6, RFC 3775 (2004)
2. Le, F., Patil, B., Perkins, C., and Faccin, C.: Diameter Mobile IPv6 Application, Internet-Draft (2004)
3. Aboba, B. and Beadles, M.: The Network Access Identifier, RFC 2486 (1999)
4. Laat, C. de, Gross, G., Gommans, L. Vollbrecht, J., and Spence, D.: Generic AAA Architecture, RFC 2903 (2000)
5. Glass, S., Hiller, T., Jacobs, S., and Perkins, C.: Mobile IP Authentication, Authorization, and Accounting Requirements, RFC 2977 (2000)
6. Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301 (2005)
7. Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and Wright T.: Transport Layer Security (TLS) Extensions, RFC 3546 (2003)
8. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and Arkko, J.: Diameter Base Protocol, RFC 3588 (2003)
9. Kwon, T., Gerla, M., Das, S., and Das, S.: Mobility Management for VoIP Service: Mobile IP vs. SIP, IEEE Wireless Communications (2002) 66-75
10. Fathi, H., Prasad, R., and Chakraborty, S.: Mobility Management for VoIP in 3G Systems: Evaluation of Low-Latency Handoff Schemes, IEEE Wireless Communications (2005) 96-104
11. Koodli, R.: Fast Handovers for Mobile IPv6, RFC 4068 (2005)
12. Soliman, H., Castelluccia, C., Malki, K., and Bellier, L.: Hierarchical Mobile IPv6 Mobility Management (HMIPv6), RFC 4140 (2005)