New Authorizing Binding to Reduce Binding Latency during Mobile IPv6 Handover Procedure

Pyung-Soo Kim and Jin-Soo Han

Department of Electronics Engineering, Korea Polytechnic University,
Siheung-City, Kyonggi-Do, 429-793, Korea

Summary
This paper proposes the new authorizing binding mechanism to reduce the binding latency between the mobile node and the correspondent node during Mobile IPv6 handover procedure. The tradeoff between security and QoS during Mobile IPv6 handover procedure is discussed. In the proposed mechanism, the authorizing binding is performed before actual handover for candidate networks where the mobile node can be attached newly, which can reduce the binding latency and thus enhance throughput degradation caused by the bidirectional tunneling. For the new authorizing binding mechanism, the return routability procedure and binding update/ack procedure are defined newly with parameters specified by information on candidate networks. In addition, cryptographic functions of authentication and encryption are also defined newly. Via experiments, it will be shown that the proposed mechanism outperforms the existing ones in terms of the L3 handover latency.

Key words:
Mobile IPv6, Authorizing binding, Handover latency, Binding latency, Security, QoS.

1. Introduction

The L3 handover latency in Mobile IPv6 [1]-[4] is caused mainly by the movement detection latency, the new CoA configuration latency and the authorizing binding latency as shown in Figure 1. These latencies are inevitable in Mobile IPv6 because of its basic operations. But the combined latency could be appreciable for real-time applications and throughput sensitive applications. Until now, there are many efforts to reduce latency, especially in movement detection phase and in new CoA configuration phase [5]-[10].

Although packet loss between the mobile node (MN) and the correspondent node (CN) can be minimized during the Mobile IPv6 handover procedure using existing fast handover mechanisms [5]-[10], the bidirectional tunneling via the home agent cannot be avoided before the binding procedure is completed between two nodes. As shown in [1]-[10], the bidirectional tunneling via the home agent does not allow the shortest communications path to be used, which can cause end-to-end delay between two nodes. In addition, this can also cause congestion at the home agent and home link. Moreover, the impact of any possible failure of the home agent or networks on the path to or from it can increase. Therefore, even if no packet loss may occur, two nodes suffer from significant throughput degradation caused by the bidirectional tunneling. That is, the binding procedure using cryptographic functions can help secure the Mobile IPv6 communication between two nodes, but it also introduces significant quality of service (QoS) issues such as delay, congestion, etc. This means there is a tradeoff between security and QoS.

In order to resolve above problem, the authorizing binding mechanism between MN and CN should be completed within short time as possible. However, as shown in [1]-[10], the return routability procedure and the binding update/ack procedure for the authorizing binding mechanism are somewhat time-consuming and computationally burdensome since cryptographic functions for authentication and encryption require considerable computation time and amount, which might introduces the binding latency. This would be serious when MN or CN is an embedded mobile platform whose processing capability, power and resource are limited. To the authors' knowledge, there seems to be no research effort on the common binding mechanism to reduce the binding latency. Therefore, in this paper, the new authorizing binding mechanism is proposed to reduce the binding latency between two nodes during the Mobile IPv6 handover procedure.

In the proposed mechanism, the authorizing binding is performed in advance for candidate networks where the MN can be attached newly, before actual handovers. That is, the return routability procedure and the binding update/ack procedure for the authorizing binding will not be performed in actual Mobile IPv6 handover procedure. Therefore, the proposed mechanism can reduce the binding latency between two nodes during the Mobile IPv6 handover procedure, and thus enhance throughput

degradation caused by the bidirectional tunneling. For the proposed authorizing binding mechanism, the return routability procedure and binding update/ack procedure are defined newly with parameters specified by information on candidate networks. In addition, cryptographic functions of authentication and encryption are also defined newly.

Finally, to verify the proposed mechanism, experiments are performed for a testbed with a single local CN communicating with the MN. For this testbed, a VoIP with G.723 voice codec is applied for the proposed mechanism and the existing fast handover mechanism [6] and then the L3 handover latency is measured. From results, it will be shown that the proposed mechanism can outperform the existing one.

The paper is organized as follows. In Section 2, the tradeoff between security and QoS in Mobile IPv6 is discussed briefly. In Section 3, the new return routability procedure and its cryptographic functions are proposed In Section 4, the binding update/ack procedure and its cryptographic functions are proposed. In Section 5, the operation procedure of the proposed mechanism is given. In Section 6, experiments are performed. Finally, conclusions are made in Section 7.

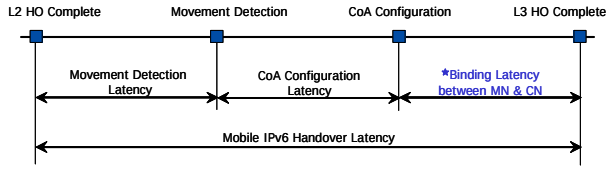

Figure 1. Mobile IPv6 Handover Latency

2. Tradeoff between Security and QoS in Mobile IPv6

As shown in [1]-[10], during Mobile IPv6 handover procedure, the bidirectional tunneling via the home agent cannot be avoided before the binding procedure is completed between MN and CN. The bidirectional tunneling via the home agent does not allow the shortest communications path to be used, which can cause end-to-end delay between two nodes. For example, a VoIP application is much more sensitive to delays than its traditional data counterparts. A few seconds' slowdown is negligible for downloading a file. However, a mere 150-millisecond delay can turn a crisp VoIP call into a garbled, unintelligent mess. In addition, this can also cause congestion at the home agent and home link. Moreover, the impact of any possible failure of the home agent or networks on the path to or from it can increase.

Therefore, even if no packet loss may occur using existing fast handover mechanisms [5]-[10], two nodes suffer from significant throughput degradation caused by the bidirectional tunneling before the authorizing binding procedure is completed. That is, the binding procedure using cryptographic functions can help secure the Mobile IPv6 communication between two nodes, but it also introduces significant QoS issues such as delay, congestion, etc. This means there is a tradeoff between security and QoS.

In order to resolve above problem, the authorizing binding between two nodes should be completed within short time as possible. To the authors' knowledge, there seems to be no research effort on the common binding mechanism to reduce the binding latency. Therefore, in this paper, the new authorizing binding mechanism is proposed to reduce the binding latency between two nodes during the Mobile IPv6 handover procedure.

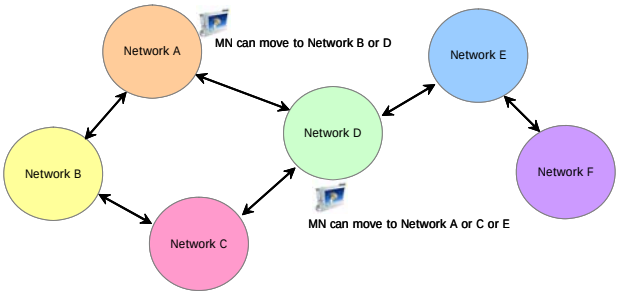

Figure 2. Mobile IPv6 based Access Networks

Network	NID	Network Prefix	Candidate Networks
A	0x01	3ffe:2e01:2a:101	B, D
B	0x02	3ffe:2e01:2a:102	A, C
C	0x03	3ffe:2e01:2a:103	B, D
D	0x04	3ffe:2e01:2a:104	A, C, E
E	0x05	3ffe:2e01:2a:105	D, F
F	0x06	3ffe:2e01:2a:106	E

Figure 3. Information on Access Networks

3. New Return Routability Procedure

This paper considers the Mobile IPv6 based access networks as shown in Figure 2. In this paper, it is assumed that all access routers (ARs) can share information on candidate networks where the MN can be attached newly. This information includes network prefixes, network identifiers (NIDs) of candidate networks as shown in Figure 3. The MN is assumed to acquire this information on candidate networks from a specific message which will not be defined in this paper.

In this section, the new return routability procedure is defined with parameters specified by network information on candidate networks. In addition, cryptographic functions of authentication and encryption are also defined newly for the new return routability procedure.

3.1 Four Messages for New Return Routability Procedure

Four messages for the new return routability procedure are defined with parameters specified by network information on candidate networks where the MN can be attached newly.

The MN sends a Home Test Init (HoTI) message to the CN (via the home agent) to acquire the home keygen token for candidate networks. The contents of the message can be summarized as follows:

- Source Address = home address
- Destination Address = correspondent
- Parameters for candidate networks :
  - NIDs
  - care-of addresses
  - home init cookies

The MN generates home init cookies and care-of addresses for candidates networks and then includes them in HoTI message as parameters.

The MN sends a Care-of Test Init (CoTI) message to the CN (directly, not via the home agent) to acquire the care-of keygen token for candidate networks. The contents of this message can be summarized as follows:

- Source Address = care-of address
- Destination Address = correspondent
- Parameters for candidate networks :
  - NIDs
  - care-of addresses
  - care-of init cookies

The MN generates care-of init cookies and care-of addresses for candidate networks and then includes them in CoTI message.

The Home Test (HoT) message is sent in response to a HoTI message. It is sent via the home agent. The contents of the message are:

- Source Address = correspondent
- Destination Address = home address
- Parameters for candidate networks :
  - NIDs
  - home init cookies
  - home keygen tokens
  - home nonce indices

Home init cookies from the MN are returned in the HoT message, to ensure that the message comes from a node on the route between the home agent and the CN. Home nonce indices are delivered to the MN to later allow the CN to efficiently find the nonce value that it used in creating home keygen tokens. The CN generates home init cookies, home keygen tokens and home nonce indices for candidate networks and then includes them in HoT message as parameters. The cryptic function to obtain home keygen tokens is shown in the following subsection.

The Care-of Test (CoT) message is sent in response to a CoTI message. This message is not sent via the home agent, it is sent directly to the MN. The contents of the message are:

- Source Address = correspondent
- Destination Address = home address
- Parameters for candidate networks :
  - NIDs
  - care-of init cookies
  - care-of keygen tokens
  - care-of nonce indices

Care-of nonce indices are provided to identify the nonce used for care-of keygen tokens. Home and care-of nonce indices may be the same, or different, in HoT and CoT messages. The CN generates care-of init cookies, care-of keygen tokens, care-of nonce indices for candidate networks and then includes them in CoT as parameters. The cryptic function to obtain care-of keygen tokens is shown in the following subsection.

3.2 Processing Cryptographic Functions for New Return Routability Procedure

In HoT and CoT messages, nonces are random numbers used internally by the CN in the creation of keygen tokens related to the return routability procedure. The nonces are not specific to a MN, and are kept secret within the CN. The CN generates nonces as the number of NIDs and each nonce is identified by a nonce index. It is assumed to keep nonces (identified by nonce indices) acceptable for two nodes are binding after it has been first used in constructing a return routability message response. The CN has a secret key (Kcn) which must be a random number, 20 octets in length. The CN generates secret keys as the number of NIDs and the life time of Kcn should be same as a nonce, so that nonce index can identify both the nonce and the Kcn.

Using the nonce and the Kcn, the keygen token (Kgt) is generated by the CN in the return routability procedure to enable the MN to compute the necessary binding management key for binding update and ack procedure. The care-of Kgt is sent by the CN in the CoT message. The home Kgt is sent by the CN in the HoT message.

When the CN receives the HoTI message, it generates home keygen tokens for candidate networks. The home Kgt_{NID} for the corresponding NID is computed as follows:

$$Home\ Kgt_{NID} = Fisrt\left[64,\ HMAC\_SHA1\left(Kcn_{NID}, (HoA \mid Nonce^{\alpha}_{NID} \mid 0)\right)\right]$$

where | denotes concatenation. This concatenation is to indicate bytewise concatenation, as in A|B, and requires that all of the octets of the datum A appear first in the result, followed by all of the octets of the datum B. A functional form "First (size, input)" is to indicate truncation of the "input" data so that only the first "size" bits remain to be used. The final "0" inside the HMAC_SHA1 function is a single zero octet, used to distinguish home and care-of cookies from each other. $Nonce^{\alpha}_{NID}$ is the HoTI nonce for the corresponding NID with the home nonce index α.

When the CN receives the CoTI message, it generates care-of keygen tokens for candidate networks. The care-of Kgt_{NID} for the corresponding NID is computed as follows:

$$Care\text{-}of\ Kgt_{NID} = Fisrt\left[64,\ HMAC\_SHA1\left(Kcn_{NID}, (CoA_{NID} \mid Nonce^{\beta}_{NID} \mid 1)\right)\right]$$

where the final "1" inside the HMAC_SHA1 function is a single octet containing the hex value 0x01, and is used to distinguish home and care-of cookies from each other. The care-of Kgt_{NID} is formed from the first 64 bits of the MAC, and sent directly to the MN at its care-of address. The care-of init cookie from the CoTI message is returned to ensure that the message comes from a node on the route to the CN. $Nonce^{\beta}_{NID}$ is the HoTI nonce for corresponding NID with the care-of nonce index β.

4. New Binding Update and Ack Procedure

When the MN has received both the HoT and CoT messages, the return routability procedure is completed. And then, the binding update and ack procedure is performed between MN and CN for the authorizing binding. Therefore, in this section, the new binding update and ack procedure is defined with parameters specified by network information on candidate networks where the MN can be attached newly. In addition, cryptographic functions of authentication and encryption are also defined newly for the new binding update and ack procedure.

4.1 Binding Update and Ack

The MN sends the binding update message to the CN directly. The contents of the binding update include the following:

- Source Address = care-of address
- Destination Address = correspondent
- Parameters for candidate networks :
  - NIDs
  - home address
  - sequence number
  - home nonce indices
  - care-of nonce indices
  - binding update keys

The binding update contains home and care-of nonces, indicating to the CN which nonces to use to compute the binding management key. The MN generates binding update keys as the number of NIDs for candidate networks and then includes them in the binding update message as parameters. The cryptic function to obtain binding update keys is shown in the following subsection.

The binding update is in some cases acknowledged by the CN. The contents of the binding ack message are as follows:

- Source Address = correspondent
- Destination Address = care-of address
- Parameters for candidate networks :
  - NIDs
  - sequence number
  - binding ack keys

The CN generates binding ack keys as the number of NIDs for candidate networks and then includes them in the binding ack message. The cryptic function to obtain binding ack keys is shown in the following subsection.

4.2 Processing Cryptographic Functions for Binding Update and Ack Procedure

When the return routability procedure is complete, the MN hashes the tokens together to form a 20 octet binding management keys for candidate networks. The binding management key (Kbm_{NID}) for the corresponding NID is computed as follows:

$$Kbm_{NID} = SHA1\left(Home\ Kgt_{NID} \mid Care\text{-}of\ Kgt_{NID}\right)$$

Kbm_{NID} is a key used for the binding update and ack procedure of corresponding NID. The return routability procedure provides a way to create a binding management key. A binding update may also be used to delete a previously established binding. In this case, the care-of Kgt_{NID} is not used. Instead, the Kbm_{NID} for the corresponding NID is generated as follows:

$$Kbm_{NID} = SHA1\left(Home\ Kgt_{NID}\right)$$

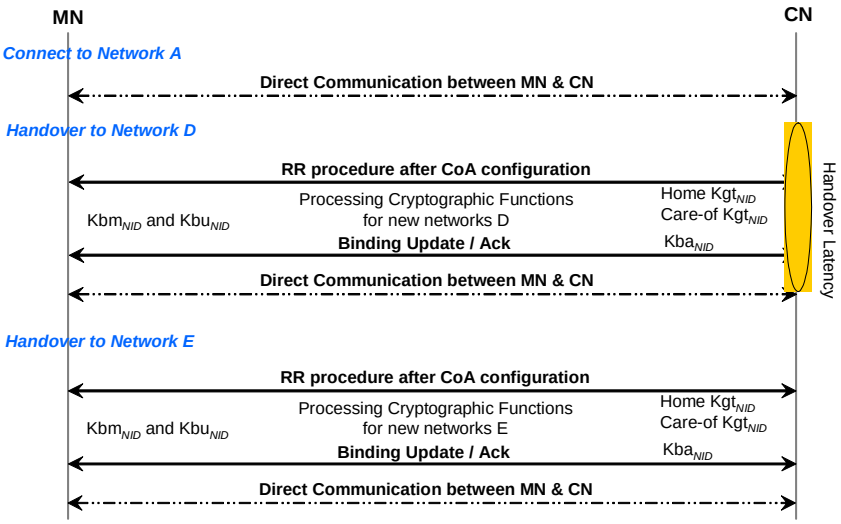

Figure 4. Operation Procedure for Existing Mechanism [1]

In the binding update and ack procedure, binding update keys and binding ack keys are required as the number of NIDs, respectively. The binding update key (Kbu_{NID}) for the corresponding NID is computed as follows:

$$Kbu_{NID} = Fisrt\left[96,\ HMAC\_SHA1\left(Kbm_{NID}, (CoA_{NID} \mid CN \mid BU)\right)\right]$$

and the binding ack key (Kba_{NID}) for the corresponding NID is computed as follows:

$$Kba_{NID} = Fisrt\left[96,\ HMAC\_SHA1\left(Kbm_{NID}, (CoA_{NID} \mid CN \mid BA)\right)\right]$$

5. Operation Procedure and Advantages over Existing Mechanism

To describe the operation procedure of the proposed mechanism, it will be assumed that the MN moves from the home network 'Network A' to the 'Network D' and then moves to the 'Network E'. The existing mechanism was explained in [1]-[10] as shown in Figure 4.

For the proposed mechanism as shown in Figure 5, when the MN is on the 'Network A', the MN and CN performs the new return routability procedure for candidate networks 'Network B' and 'Network D' at appropriate time using information such as network prefixes, NIDs of Figure 3. When the MN performs actual Mobile IPv6 handover to 'Network D', the direct communication between MN and CN can be started without the authorizing binding procedure after the CoA configuration on 'Network D'. This can make fast authorizing binding between two nodes because somewhat time-consuming and computationally burdensome tasks are performed beforehand. On the other hand, in the existing mechanism [1]-[10], these time-consuming and computationally burdensome tasks for authorizing binding are performed during the Mobile IPv6 handover procedure. Therefore, the proposed mechanism can reduce the binding latency between two nodes during the Mobile IPv6 handover procedure and thus enhance throughput degradation caused by the bidirectional tunneling.

6. Experiments

In this section, to evaluate the proposed mechanism, experiments are performed for a testbed where there are two candidate networks, and a single CN communicating with the MN. Both MN and CN are embedded mobile handheld platforms that have limited CPU performance and resources. As an application for experiments, a VoIP with G.723 voice codec is applied for the proposed mechanism and the existing fast handover mechanism [6]. And then the L3 handover latency is measured from L2 trigger to binding CoA with CN. To make a clearer comparison, 10 experiments are performed, and 20 handovers for each single experiment are occurred. For two mechanisms, results are shown in Table 1 for L3 handover latency. It can be shown that the proposed mechanism outperforms the existing one [6].

Table 1 Mean values of handover latency

Proposed Mechanism	Existing Mechanism [6]
461 msec	574 msec

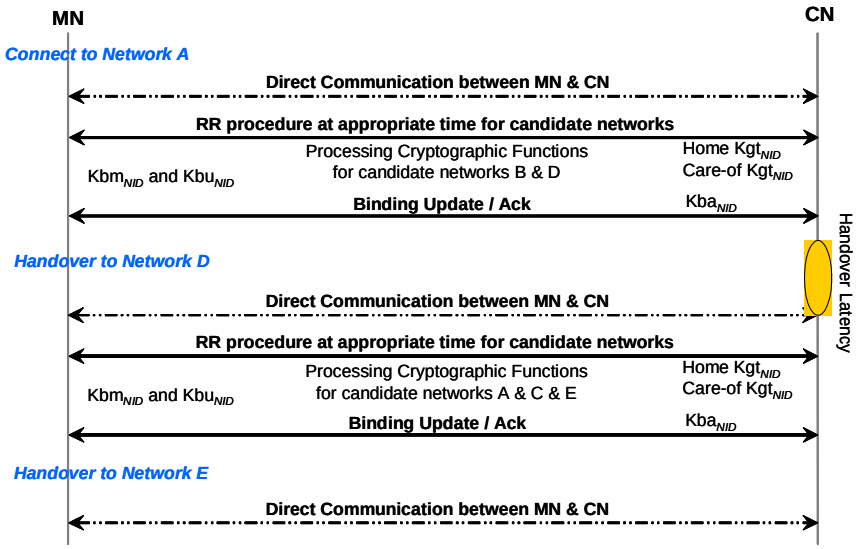

Figure 5. Operation Procedure for Proposed Mechanism

7. Conclusions

This paper has proposed the new authorizing binding mechanism to reduce the binding latency between MN and CN during Mobile IPv6 handover procedure. The tradeoff between security and QoS during Mobile IPv6 handover procedure is briefly discussed. In the proposed mechanism, the authorizing binding is performed before actual handover for candidate networks where the mobile node can be attached newly, which can reduce the binding latency and thus enhance throughput degradation caused by the bidirectional tunneling. For the new authorizing binding mechanism, the return routability procedure and binding update/ack procedure are defined newly with parameters specified by information on candidate networks. In addition, cryptographic functions of authentication and encryption are also defined newly. Via experiments, it has been shown that the proposed mechanism outperforms the existing one in terms of the L3 handover latency.

Acknowledgement

This work was financially supported by National Security Research Institute (NSRI) in Electronics and Telecommunications Research Institute (ETRI) of Korea.

References

[1] Johnson, D.B., Perkins, C.E., Arkko, J.: Mobility Support in IPv6. IETF RFC 3775 (June 2004)

[2] Costa, X.P., Hartenstein, H.: A simulation study on the performance of mobile IPv6 in a WLAN-based cellular network. Computer Networks 40 (2002) 191~204

[3] Vaughan-Nichols, S.J.: Mobile IPv6 and the future of wireless internet access. Computer 36 (2003) 18~20

[4] Pramil, A.D., Antoine, S., Aghvami, A.H.: Enhanced tcp performance over mobile IPv6: innovative fragmentation avoidance and adaptive routing techniques. In: First IEEE Consumer Communications and Networking Conference. (2004) 175~180

[5] Kempf, J., Wood, J., Fu, G.: Fast Mobile IPv6 handover packet loss performance: measurement for emulated real time traffic. In: 2003 IEEE Wireless Communications and Networking. (2003) 1230~1235

[6] Koodli, R.: Fast Handovers for Mobile IPv6. IETF RFC 4068 (July 2005)

[7] Y. Gwon, A. Yegin, "Enhanced Forwarding From Previous Care-of Address For Fast Mobile IPv6 Handovers (eFWD)", IETF Draft : draft-gwon-mobileip-efwd-fmipv6-01.txt, Jan 2003.

[8] A. Yegin et al., "Link-layer Event Notifications for Detecting Network Attachments", IETF Draft : draft-ietf-dna-link-information-03.txt (Oct 2005)

[9] McCann, P.: Mobile IPv6 Fast Handovers for 802.11 Networks. IETF RFC 4260 (November 2005)

[10] Kim, P.S., Lee, Y.S., Park, S.: New fast handover mechanism for mobile ipv6 in IEEE 802.11 wireless networks. Lecture Notes in Computer Science 3320 (2004) 641~644

Pyung-Soo Kim He received the B.S. degree in Electrical Engineering from Inha University in 1994. He received the M.S. degree in Control and Instrumentation Engineering and the Ph.D. degree at the School of Electrical Engineering and Computer Science from Seoul National University in 1996 and

2001, respectively. From 2001 to 2005, he was a senior researcher at the Digital Media R&D Center of Samsung Electronics Co. Ltd. Since 2005, he has been with the Department of Electronics Engineering at Korea Polytechnic University. His main research interests are in the areas of system software solutions, wireless mobile networks, next generation network system design, statistical signal processing, and various industrial applications.

Jin-Soo Han He received his B.S degree of Electronics Engineering from Korea University in 1986 and M.S. degree from N.Y. Polytech. in 1993 and Ph.D. degree from Myoung Ji University in 2003 respectively. He has been an Assistant Professor of Electronics Engineering Department, Korea Polytechnic University since March 2000. His research area includes communication, signal processing, and data compression.