IEICE TRANS. INF. & SYST., VOL.E93–D, NO.5 MAY 2010

PAPER Special Section on Information and Communication System Security

ESS-FH: Enhanced Security Scheme for Fast Handover in Hierarchical Mobile IPv6

Ilsun YOU[†a)], **Jong-Hyouk LEE**[††], **Kouichi SAKURAI**[†††], *and* **Yoshiaki HORI**[†††], *Members*

SUMMARY Fast Handover for Hierarchical Mobile IPv6 (F-HMIPv6) that combines advantages of Fast Handover for Mobile IPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6) achieves the superior performance in terms of handover latency and signaling overhead compared with previously developed mobility protocols. However, without being secured, F-HMIPv6 is vulnerable to various security threats. In 2007, Kang and Park proposed a security scheme, which is seamlessly integrated into F-HMIPv6. In this paper, we reveal that Kang-Park's scheme cannot defend against the Denial of Service (DoS) and redirect attacks while largely relying on the group key. Then, we propose an Enhanced Security Scheme for F-HMIPv6 (ESS-FH) that achieves the strong key exchange and the key independence as well as addresses the weaknesses of Kang-Park's scheme. More importantly, it enables fast handover between different MAP domains. The proposed scheme is formally verified based on BAN-logic, and its handover latency is analyzed and compared with that of Kang-Park's scheme.

key words: *F-HMIPv6 security, CGA, BAN-logic*

1. Introduction

Mobile IPv6 (MIPv6) is a protocol that provides mobility service for a mobile node (*MN*) regardless of its movements in IPv6 networks [1]. In spite of its great potential, it suffers from long handover latency and high signaling overhead. In order to address these problems, FMIPv6 [2] and HMIPv6 [3] have been proposed. While FMIPv6 improves the handover latency through link layer (L2) triggers and bi-directional tunneling between access routers (*AR*s), HMIPv6 optimizes the signaling overhead by adopting a local home agent (*HA*) called Mobility Anchor Point (*MAP*). These two enhancements adopt their own different approaches to improve MIPv6. It is thus natural that there is a high need to gracefully combine them together to take all their advantages. As a result, F-HMIPv6 has been developed [4], [5]. It is well known that this enhancement successfully achieves the best performance in terms of handover latency and signaling overhead [6].

Despite the best efficiency, without being secured, F-HMIPv6 is vulnerable to various security threats such as the DoS or redirect attacks [7], [8]. Recently, Kang and Park proposed a security scheme to provide secure handovers for F-HMIPv6 [8]. To our best knowledge, this is the only security scheme properly harmonized with F-HMIPv6. Thus, it has played a milestone role for the security of F-HMIPv6. However, we discover that Kang-Park's scheme is still vulnerable to the DoS and redirect attacks while largely depending on the group key. Additionally, in Kang-Park's scheme, the fast handover cannot be supported when *MN*s move between different MAP domains. In this paper, we analyze its weaknesses, and then propose an Enhanced Security Scheme for F-HMIPv6 (ESS-FH). Based on the *Cryptographically Generated Address (CGA)* method [9] and the public key cryptography, ESS-FH provides the strong key exchange and the key independence in addition to improving the weaknesses, from which Kang-Park's scheme suffers. Moreover, it achieves the secure fast inter-handover between different MAP domains.

The reminder of the paper is organized as follows: In Sect. 2, we describe Kang-Park's scheme and analyze its weaknesses. In Sect. 3, we introduce the enhanced security scheme for F-HMIPv6 by splitting three operations: initialization, intra-handover, and inter-handover phases. BAN-logic based security analysis is given in Sect. 4. Then, in Sect. 5, the analytical modeling for handover latency and its numerical results are presented prior to the conclusions in Sect. 6.

2. Kang-Park's Security Scheme

Kang-Park's scheme is composed of two phases: MAP registration phase and handover phase. While the first phase is performed when an *MN* bootstraps or moves in a new MAP domain, the second one is executed when the *MN* moves between *AR*s within the MAP domain. In order to protect the MAP registration phase, Kang-Park's scheme leverages the Authentication, Authorization, and Accounting (AAA) infrastructure [10], through which a *MAP* shares a session key with an *MN* as well as authenticates it. Especially, the *MAP* issues a ticket to the *MN* to safely deliver the session key to its *AR*s. For this goal, it is assumed that the *MAP* shares a group key with its *AR*s in advance, and all involved nodes are time-synchronized. Note that the group key is used to encrypt the session key and the encrypted key is included in the ticket. Thus, once given the ticket, each *AR* can extract the session key. In the handover phase, after receiving the ticket, the *AR* recovers and uses the session key to protect the fast handover phase.

Manuscript received August 3, 2009.
Manuscript revised December 16, 2009.

[†]The author is with School of Information Science, Korean Bible University, South Korea.
[††]The author is a corresponding author and with IMARA Team at INRIA, France.
[†††]The authors are with the Dept. of Computer Science and Communication Engineering, Kyushu University, Fukuoka-shi 819–0395 Japan.
a) E-mail: isyou@bible.ac.kr

DOI: 10.1587/transinf.E93.D.1096

In spite of its seamless integration with F-HMIPv6, Kang-Park's scheme has the following weaknesses:

- **Dependency on the group key**: As mentioned above, Kang-Park's scheme depends on the group key approach to securely distribute the session key. Therefore, if the group key is revealed, this scheme becomes vulnerable to various security threats and thus can be easily attacked. Unfortunately, it is not easy to securely manage the group key because it is leaked even if only one *AR* is compromised. Also, the cost for recovering the key is expensive.
- **Denial of Service attack**: In the MAP registration phase, the *Router Advertisement (RtAdv)* message, unlike the *Local Binding Update (LBU)* and *Local Binding Acknowledgement (LBA)* ones, is not protected. This message can thus be easily forged to deceive *MN*s into believing that they have just entered the target MAP domain. If such an attack is successful, *LBU* messages are simultaneously sent to the target *MAP*. As a result, the *MAP* and the related *AR*s are occupied while suspending their meaningful jobs.
- **Redirect attack**: There are two kinds of redirect attacks: session hijacking and malicious mobile node flooding [7]. Kang-Park's scheme is vulnerable to the malicious mobile node flooding attack because, in the handover phase, the *MAP*, unlike the *nAR*, cannot detect if the *MN* truly attaches to the new network. That makes the target network to be flooded with unwanted excess traffic.

In addition, Kang-Park's scheme does not support the fast handover when *MN*s move between different MAP domains, *i.e.*, inter-handover. That makes this scheme unable to continuously guarantee the quality of service required for delay sensitive applications.

3. Enhanced Security Scheme for F-HMIPv6

In this section, the proposed ESS-FH is introduced. In ESS-FH, each *MN* negotiates a secret key *Kbm* with the *MAP* whenever moving to the MAP domain. For this *Kbm* negotiation, the public-key cryptography is applied in conjunction with the *CGA* method [9]. Based on the *Kbm*, ESS-FH achieves a seamless integration between the fast handover and the local binding update. Moreover, it allows the *MN* to continually execute the fast handover even between different MAP domains.

3.1 Notations and Preliminary

Notations used in this paper are shown in Fig. 1.

It is assumed that each entity, *i.e.*, *MN*, *AR* or *MAP*, has its own public/private key pair and its IPv6 address is a *CGA*, which is derived from its public key. For example, an *MN* has a public/private key pair PU_{MN}/PR_{MN} and its *Regional Care-of Address (RCoA)* is a *CGA*, which is generated from the PU_{MN}. Also, it is supposed that there is a

$Msg(A, B)$	the message *Msg* sent from *A* to *B*, where *A* and *B* are an IPv6 address
$E(K, M)$	a function that encrypts the message *M* with the given key *K*, where *K* can be a secret key or a public key
$S(K, M)$	a function that digitally signs the message *M* with the private key *K*
MN and *AS*	a Mobile Node and an Authentication Server respectively
AR	an Access Router and its IPv6 address (*pAR*: previous *AR*, *nAR*: new *AR*)
MAP	a Mobility Anchor Point and its IPv6 address
NAI_X	the *X*'s Network Access Identifier
GK	the group key of the *MAP* and its *AR*s
PU_X	the *X*'s public key from which the *CGA* is derived, where *CGA* denotes *Cryptographically Generated Address* [9]
PR_X	the *X*'s private key which corresponds to PU_X
$CGAP_X$	the parameters used to verify that the *X*'s CGA is derived from PU_X
$H(M)$	an one-way hash value of the message *M*
$HMAC(K, M)$	an HMAC Value computed using the secret *K* over the message *M*
|	concatenation operation

Fig. 1 Notations.

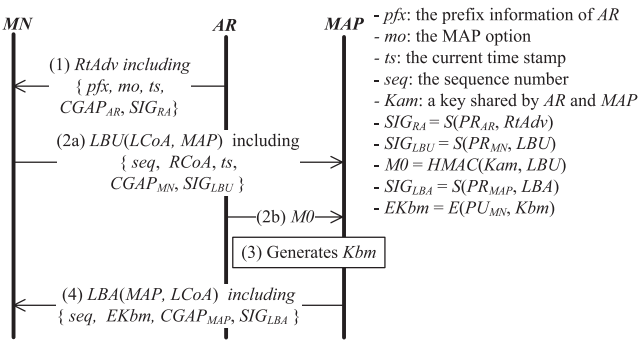

Fig. 2 Initialization phase.

secure channel between a *MAP* and an *AR*. In addition, they share a *Kam* with each other while being time-synchronized. In this paper, we only describe the predictive mode in the fast handover [2].

3.2 Operation

ESS-FH is composed of three phases: initialization, intra-handover, and inter-handover phases. The initialization phase is only once executed by an *MN* during its bootstrapping stage or during its movement from the home network. In this phase, the *MN* negotiates a secret key with its current *MAP* while performing the local binding update. After the phase, if the *MN* moves to a new network, the intra-handover phase or the inter-handover phase is performed depending on the type of handover.

3.2.1 Initialization Phase

As shown in Fig. 2, the initialization phase is composed of the *RtAdv, LBU* and *LBA* messages. These messages are protected through the *CGA* method. That is, each message includes its digital signature and related *CGA* parameters. If an entity receives a message, it verifies the sender's public key with both the sender's address and the *CGA* parameters. Then, it uses the public key to validate the received digital signature.

Let us assume that each *AR* periodically distributes the

RtAdv message to *MN*s attached to its network. Especially, it uses its private key PR_{AR} to digitally sign this message. When receiving the *Router Solicitation (RtSol)* message sent from the *MN*, it just responds with the latest *RtAdv* message instead of making a new one to prevent the DoS attacks.

Once the *MN* is turn-on, it receives the *RtAdv* message from its current *AR*. In order to authenticate this message, it verifies the attached signature SIG_{RA} with the *AR*'s public key PU_{AR}. If the message is valid, the *MN* configures both the *Local Care-of Address (LCoA)* and the *RCoA*. Note that the *RCoA* is the *CGA* derived from the *MN*'s public key PU_{MN}. Afterwards, the *MN* prepares and digitally signs the *LBU* message, which is then sent to the *MAP*. Prior to forwarding this message to the *MAP*, the *AR* adds it to $M0$ computed on it using *Kam*. Through $M0$, the *MAP* can check if the *MN* exists in the *AR*'s network. That makes it impossible for the malicious *MN* to redirect its traffic to other networks at will. When receiving the message, the *MAP* checks if the timestamp *ts* is within the current time window and $M0$ is valid. In order to prevent the DoS attacks, the expensive operation, *e.g.*, the digital signature verification, is performed only in the positive case. Thus, when the two values *ts* and $M0$ are valid, the *MAP* verifies SIG_{LBU}. If the signature is correct, the *MAP* is sure that the *MN* truly owns the given *RCoA* and PU_{MN}. More importantly, it believes the binding between the *MN*'s *RCoA* and *LCoA*. To reply the *LBU* message, the *MAP* prepares and digitally signs the *LBA* one after generating a secret key *Kbm* and encrypting it with PU_{MN}. Upon receiving the *LBA* message, the *MN* verifies the signature SIG_{MAP}, and then decrypt *EKbm* into *Kbm*. As a result of this phase, the *MAP* believes that the *MN*'s *RCoA* is associated with the *LCoA* while negotiating the secret key *Kbm* with the *MN*. Also, it believes that the *MN* indeed exists within the *AR*'s network.

3.2.2 Intra-Handover Phase

Figure 3 illustrates the intra-handover phase that is executed when the *MN* moves within its current MAP domain. In this phase, the key *Kbm*, which is negotiated during the initialization phase, is used to protect the signaling messages and distribute the secret key *Kma* between the *MN* and the new *AR*.

When the *MN* detects its movement through L2 triggers, it sends the *MAP* the *Router Solicitation for Proxy Advertisement (RtSolPr)* message protected by the authenticator $M1$. On receiving the message, the *MAP* first verifies $M1$ with the *Kbm*. If $M1$ is valid, it generates the secret key *Kma*, which is then encrypted into *EKma*. Then, the *MAP* sends the *MN* the *Proxy Router Advertisement (PrRtAdv)* message including the new *AR*'s information and its authenticator $M2$. While the former is used to configure the *MN*'s new *LCoA*, the latter is used to detect if the message is changed. If $M2$ is valid, the *MN* decrypts *EKma* into *Kma*, and then configures its new *LCoA*. Note that *Kma* is used to secure the *Unsolicited Neighbor Advertisement (UNA)* message. Once the *MN* configures its *LCoA*, it

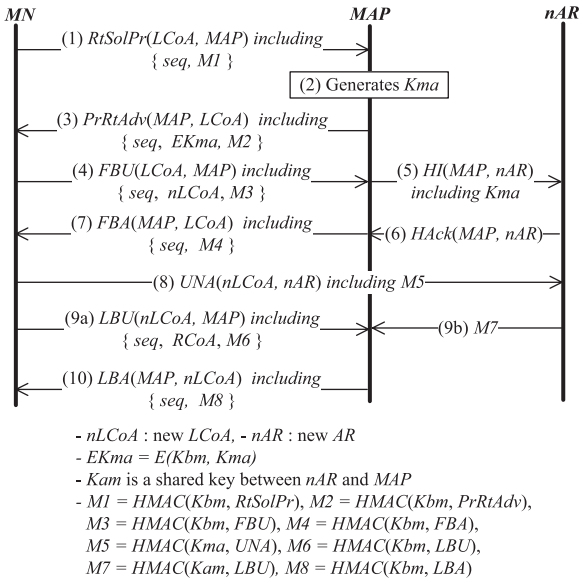

Fig. 3 Intra-handover phase.

sends the *MAP* the *Fast Binding Update (FBU)* message indicating the binding between the *MN*'s *RCoA* and *nLCoA*. Upon receipt of the *FBU* message, the *MAP* verifies the included $M3$. If $M3$ is valid, the *MAP* believes that the *MN* truly owns both the *nLCoA* and *RCoA*. With such a belief, it exchanges the *Handover Initiate (HI)* and *Handover Acknowledge (HACK)* messages with the *nAR*. During this exchange, *Kma* is delivered to the *nAR* through the *HI* message. As a result, the *MAP* starts to tunnel the traffic sent to *LCoA* to the *nAR* while returning the *MN* the *Fast Binding Acknowledge (FBA)* message. Thus, the valid *FBA* message convinces the *MN* that its data packets are being forwarded to its new location. As soon as the *MN* moves to the *nAR*'s network, it announces its attachment by sending the *UNA* message to the *nAR*. If this message is correct, the *nAR* trusts that the *MN* arrives at its network, and consequently starts to deliver the buffered data packets to the *MN*'s *nLCoA*. Afterwards, the *MN* exchanges the *LBU* and *LBA* messages with the *MAP*. At this point, if the *nAR* receives the *LBU* message from the *MN*, it computes $M7$ by using *Kam* before forwarding it to the *MAP*. Then, the computed value is sent to the *MAP* together with the message. When they arrive, the *MAP* uses $M6$ to verify the correctness of the *LBU* message asserting the binding between the *MN*'s *nLCoA* and *RCoA* while using $M7$ to check if the *MN* really exists within the *nAR*'s network. If they are all valid, the *MAP* stops the packet forwarding to the *nAR* while sending the *LBA* message to the *MN*. Note that due to $M7$, the malicious *MN*, which does not exist in the *nAR*'s network, cannot deceive the *MAP* into believing that it moves at the *nLCoA* and making that the network suffers from the redirected traffic.

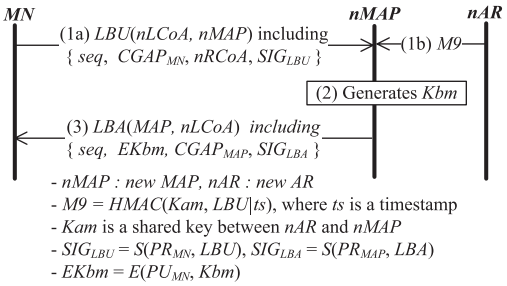

Fig. 4 Inter-handover phase.

3.2.3 Inter-Handover Phase

The inter-handover phase is performed when the *MN* moves from its current MAP domain to another. To support this phase, it is assumed that the current *MAP* shares *Kam* with the *AR*s, which do not belong to itself and are located at the boundary of its domain. Also, the *PrRtAdv* message includes a MAP option, through which the *MN* recognizes its movement between *MAP*s. When this phase starts, the *MN* first executes the (1)–(8) steps of the intra-handover one. Also, the *MAP* sends the next *seq* with the *Kma* through the *HI* message. That makes the *MN* and the *nMAP* continue to use *seq* as a fresh nonce. Once the *MN* configures its new *RCoA* after sending the *UNA* message, it exchanges the *LBU* and *LBA* messages with the *nMAP* as depicted in Fig. 4. In order to be authenticated, the messages are digitally signed with the sender's private key in the same way as being done in the initialization phase. Especially, the *LBU* message is accompanied by *M*9, which the *nAR* computes to protect the *nMAP* against both the DoS and redirect attacks. Before computing *M*9, the *nAR* verifies the *seq* included in the *LBU* message with the one which it received from the *MAP*. If the *M*9 is valid, the *nMAP* can confirm that the *MN* really exists in the *nAR*'s network as well as safely verify the digital signature SIG_{LBU} without being vulnerable to the DoS attack. Additionally, to be negotiated between the two entities, the secret key *Kbm* is encrypted with the PU_{MN} into *EKbm*, which is then conveyed in the *LBA* message.

4. Security Analysis

In this section, ESS-FH is analyzed in terms of security. For this goal, we first validate its correctness based on BAN-logic [11] and then provide discussion on its security properties.

4.1 Formal Verification

For the formal verification of the proposed protocol, we apply BAN-logic which introduced by Burrows, Abadi and Needham in 1989. Because of simplicity and robustness, BAN-logic has been one of the most popular methods for analyzing security protocols. Typically, BAN-logic is composed of the following steps: (*i*) idealizing the original protocol, (*ii*) defining assumptions about the initial state and (*iii*) applying logical postulates repeatedly until getting the intended results. For details on notations and logical postulates of BAN-logic, refer to [11].

In order to make verification more convenient, the extended rules E1–E3 are defined as follows:

$$\text{E1: } \frac{A \equiv \overset{PU_B}{\mapsto} B,\ A \triangleright \{H(M)\}_{PR_B}}{A \equiv B \mid\sim M}$$

$$\text{E2: } \frac{A \equiv \overset{PU_A}{\mapsto} A,\ A \equiv B \equiv \{M\}_{PU_A}}{A \equiv B \equiv M}$$

$$\text{E3: } \frac{A \equiv A \overset{K}{\leftrightarrow} B,\ A \equiv B \equiv \{M\}_K}{A \equiv B \equiv M}$$

It is clear from the meaning of the definitions that they are intuitively true. Also, let R1, R2, and R3 denote the message-meaning, nonce-verification, and jurisdiction rules, respectively.

4.1.1 Initialization Phase

As the first step for verification, the initialization phase is translated into the idealized version as follows:

(1-1) $AR \rightarrow MN : \{H(RtAdv)\}_{PR_{AR}}$
(1-2) $MN \rightarrow MAP : \{H(\#(seq), LBU)\}_{PR_{MN}}$
(1-3) $AR \rightarrow MAP : <LBU>_{Kam}$
(1-4) $MAP \rightarrow MN : \{H(LBA)\}_{PR_{MAP}}$
* *LBA* includes $\{MAP \overset{Kbm}{\rightleftharpoons} MN\}_{PU_{MN}}$

In order to analyze this phase, we define the following assumptions:

A11: $MN \equiv \overset{PU_{AR}}{\mapsto} AR$
A12: $MAP \equiv \overset{PU_{MN}}{\mapsto} MN$
A13: $MAP \equiv \#(ts)$
A14: $MAP \equiv MAP \overset{Kam}{\rightleftharpoons} AR$
A15: $MAP \equiv MAP \overset{Kbm}{\rightleftharpoons} MN$
A16: $MN \equiv \overset{PU_{MAP}}{\mapsto} MAP$
A17: $MN \equiv \#(seq)$
A18: $MN \equiv \overset{PU_{MN}}{\mapsto} MN$
A19: $MN \equiv MAP \Rightarrow MAP \overset{Kbm}{\rightleftharpoons} MN$

Strictly speaking, it cannot be proved from BAN-logic that the *MN* and the *MAP* own PU_{MN} and PU_{MAP}, respectively. Because of this reason, A14 and A18 are presented.

With the idealized version and the assumptions, we can analyze this phase as follows:

From (1-1), we derive:

(1) $MN \models AR \mid\sim RtAdv$ [by A11, R1]

(2) $MN \models AR \models RtAdv$ [by R2 if $MN \models \#(ts)$]

From (1-2), we derive:

(3) $MAP \models AR \models LBU$ [by A14, R1, A13, R2]

From (1-3), we derive:

(4) $MAP \models MN \models LBU$ [by A12, E1, A13, R2]

(5) $MAP \models MN \models \#(seq)$ [by (4)]

From (1-4), we derive:

(6) $MN \models MAP \models LBA$ [by A16, E1, A17, R2]

(7) $MN \models MAP \models MAP \overset{Kbm}{\rightleftharpoons} MN$ [by (6), A18, E2]

(8) $MN \models MAP \overset{Kbm}{\rightleftharpoons} MN$ [by (7), A19, R3]

If the *MN* is not time-synchronized with the *AR* and the *MAP*, it cannot say whether the *RtAdv* message is a replay or not because there is nothing in the message that it knows to be fresh. In other words, it just believes that the *AR* once sent the message. However, because the information given by the message tends to be rarely changed, we can proceed this analysis with such a belief, *i.e.*, the formula (1). If the time is synchronized, the *MN* can believe that the *AR* believes the *RtAdv* message as shown in the formula (2). On the other hand, based on the assumption A13 and the formula (3), the *MAP* can safely perform the asymmetric cryptographic operations while defending against the DoS attack. The formulas (3), (4) and (6) show that the *MN* and the *MAP* trust the local binding update performed during this phase. Especially, the formulas (3) and (4) make that the protocol being analyzed is not vulnerable to the redirection attacks. Due to the formula (5), in the subsequent phases, the *seq*'s freshness can be believed. In addition, the formula (8) gives the *MN* the belief that it successfully shares *Kbm* with the *MAP*. Therefore, we can conclude that this phase is correct.

4.1.2 Intra-Handover Phase

The intra-handover phase is idealized into the following version:

(2-1) $MN \rightarrow MAP : <RtSolPr>_{Kbm}$

(2-2) $MAP \rightarrow MN : <PrRtAdv>_{Kbm}$

(2-3) $MN \rightarrow MAP : <FBU>_{Kbm}$

(2-4) $MAP \rightarrow MN : <FBA>_{Kbm}$

(2-5) $MN \rightarrow nAR : <UNA,\ \#(MN \overset{Kma}{\rightleftharpoons} nAR)>_{Kma}$

(2-6) $MN \rightarrow MAP : <LBU>_{Kbm}$

(2-7) $nAR \rightarrow MAP : <LBU>_{Kam}$

(2-8) $MAP \rightarrow MN : <LBA>_{Kbm}$

* *seq* is included in all messages except for *UNA*
PrRtAdv includes $\{MN \overset{Kma}{\rightleftharpoons} nAR\}_{Kbm}$

In this form, the $HMAC(K, M)$ is expressed as $< M >_K$. Also, *Kma* is included as a nonce in (2-5) because it is newly generated by the *MAP*. Note that all messages except for the *UNA* message contain *seq* as a nonce.

The assumptions are given as follows:

A21: $MAP \models \#(seq)$
A22: $MAP \models MAP \overset{Kbm}{\leftrightarrow} MN$
A23: $MAP \models MAP \overset{Kbm}{\rightleftharpoons} MN$
A24: $MAP \models MAP \overset{Kam}{\rightleftharpoons} nAR$
A25: $nAR \models MAP \overset{Kam}{\rightleftharpoons} nAR$
A26: $nAR \models MN \overset{Kma}{\rightleftharpoons} nAR$
A27: $nAR \models \#(MN \overset{Kma}{\rightleftharpoons} nAR)$
A28: $MN \models \#(seq)$
A29: $MN \models MAP \overset{Kbm}{\leftrightarrow} MN$
A2a: $MN \models MAP \overset{Kbm}{\rightleftharpoons} MN$
A2b: $MN \models MAP \mapsto MN \overset{Kma}{\rightleftharpoons} nAR$

Note that the four assumptions (A22, A23, A29, and A2a) are provided together because the *Kbm* plays two roles of both the shared secret and the encryption key. Also, the *nAR* can believe the *Kma* and its freshness since it safely receives the secret from the *MAP* through their secure channel. Thus, the assumptions (A26 and A27) are added.

Once we have the idealized form and the assumptions, we can verify this phase as follows:

From (2-1) and (2-2), we derive:

(1) $MAP \models MN \models PrRtSol$ [by A23, R1, A21, R2]

(2) $MN \models MAP \models PrRtAdv$ [by A2a, R1, A28, R2]

(3) $MN \models MN \overset{Kma}{\rightleftharpoons} nAR$ [by (2), A29, E3, A2b, R3]

From (2-3) and (2-4), we derive:

(4) $MAP \models MN \models FBU$ [by A23, R1, A21, R2]

(5) $MN \models MAP \models FBA$ [by A2a, R1, A28, R2]

From (2-5), we derive:

(6) $nAR \models MN \models UNA$ [by A26, R1, A27, R2]

From (2-6), (2-7) and (2-8), we derive:

(7) $MAP \models MN \models LBU$ [by A23, R1, A21, R2]

(8) $MAP \models nAR \models LBU$ [by A24, R1, A21, R2]

(9) $MN \models MAP \models LBA$ [by A2a, R1, A28, R2]

Note that the *nAR* trusts the *MN*'s attachment based on the formula (6). With such a trust, the *nAR* forwards the *LBU* message with the *M*7, leading to the formula (8). Thus, the formula (8) makes the *MAP* confirms that the *MN* is present at the *nAR*'s network. By the formulas (4), (7), and (8), we can know that the *MAP* has reasonable beliefs about the *FBU* and *LBU* messages. As a result, it can be concluded that this phase is valid.

4.1.3 Inter-Handover Phase

As mentioned above, the inter-handover phase is the same as the intra-handover one before the local binding update. Thus, we focus on the local binding update to verify this phase. The idealized version of this phase is as follows:

(3-1) $nAR \rightarrow nMAP : <\#(seq), ts, LBU>_{Kam}$

(3-2) $MN \rightarrow nMAP : \{H(LBU)\}_{PR_{MN}}$

(3-3) $nMAP \rightarrow MN : \{H(LBA)\}_{PR_{nMAP}}$

* *LBA* includes $\{MN \overset{Kbm}{\rightleftharpoons} nMAP\}_{PU_{MN}}$
LBU and *LBA* include *seq*

The assumptions are defined as follows:

A31: $nMAP \models nMAP \overset{Kam}{\rightleftharpoons} nAR$
A32: $nMAP \models \#(ts)$
A33: $nMAP \models nAR \Rightarrow \#(seq)$
A34: $nMAP \models \overset{PU_{MN}}{\mapsto} MN$
A35: $nMAP \models nMAP \overset{Kbm}{\rightleftharpoons} MN$
A36: $MN \models \overset{PU_{nMAP}}{\mapsto} nMAP$
A37: $MN \models \#(seq)$
A38: $MN \models \overset{PU_{MN}}{\mapsto} MN$
A39: $MN \models nMAP \Rightarrow nMAP \overset{Kbm}{\rightleftharpoons} MN$

From this point, we proceed to validate this phase.

From (3-1) and (3-2), we derive:

(1) $nMAP \models nAR \models LBU$ [by A31, R1, A32, R2]
(2) $nMAP \models \#(seq)$ [by (1), A33, R3]
(3) $nMAP \models MN \models LBU$ [by A34, E1, (2), R2]

From (3-3), we derive:

(4) $MN \models nMAP \models LBA$ [by A36, E1, A37, R2]
(5) $MN \models nMAP \models nMAP \overset{Kbm}{\leftrightarrow} MN$ [by (4), A38, E2]
(6) $MN \models nMAP \overset{Kbm}{\leftrightarrow} MN$ [by (5), A39, R3]

Based on the formulas (1) and (2), the *nMAP* can trust the binding between the *MN*'s *nLCoA* and *nRCoA*. Especially, the formula (1) enables the *nMAP* to guard against the DoS and redirect attacks. In addition, through the formula (5), the *MN* is sure that it successfully negotiates the *Kbm* with the *nMAP*. Consequently, we can conclude that this phase is correct.

4.2 Security Properties

(1) Secure key exchange: In ESS-FH, two keys *Kbm* and *Kma* are exchanged during the handover. When the *MN* executes the initialization phase or the inter-handover one, it exchanges the *Kbm* with the new *MAP* based on the public key encryption. That is, the *MAP* encrypts the *Kbm* with the *MN*'s public key PU_{MN}, and then sends the encrypted value *EKbm* to the *MN*. In order to safely use the public key method, the *MAP* verifies the PU_{MN} through the *CGA* method, which requires no third parties or additional infrastructure, such as a public-key infrastructure, to prove the address ownership [9]. Once the *Kbm* is negotiated, the *MN* uses it to efficiently exchange the *Kma* with the new *AR* whenever moving within the MAP domain. In this way, ESS-FH achieves secure key exchange based on both the public key encryption and the *CGA* method. Note that the AAA infrastructure can be used instead of the public key system [10]. However, compared to the AAA infrastructure, it enables handovers between *MAPs*, *i.e.*, the inter-handover phase, to be more efficiently executed without the involvement of the *AS*.

(2) Key independence: In ESS-FH, the *MN* makes use of *Kbm* to share a new *Kma* with a new *AR* whenever moving within its current MAP domain. Similarly, in order to move between *MAPs*, it negotiates a new *Kbm* with a new *MAP* based on the public key encryption. Therefore, even if the current *Kbm* or *Kam* is compromised, its previous or successive keys are not compromised.

(3) Preventing Redirect attacks: As mentioned above, the redirect attacks can be divided into two types: session hijacking and malicious mobile node flooding. In F-HMIPv6, the adversary can launch the session hijacking attack by deceiving the current *MAP* into redirecting a victim node's network traffic to itself through the false *LBU* or *FBU* message. ESS-FH is not vulnerable to this attack because the binding update message is strongly authenticated based on the digital signature SIG_{LBU} or the HMAC value $M3$. On the other hand, the malicious mobile node flooding attack can be launched in a way that a malicious *MN* sends its *MAP* a false binding update message, arguing it moves to a victim node's address. Because the *MN* is a legitimate node, the digital signature or HMAC value attached to the binding update message is valid. As a result, the *MAP* accepts the message, thus redirecting the *MN*'s network traffic to the victim node. In ESS-FH, each *LBU* message should be accompanied by its HMAC value, which the current *AR* computes with *Kam*. Based on the HMAC value, the *MAP* can believe that the *MN* indeed exists within the *AR*'s network. Consequently, ESS-FH is not vulnerable to the malicious mobile node flooding attack.

(4) Preventing Denial of Service attacks: Because ESS-FH adopts the public key method to protect the *LBU* and *LBA* messages, the adversary can launch the DoS attack by sending a big storm of the *LBU* messages to the target *MAP*. In order to address this problem, ESS-FH allows the *MAP* to verify the values *ts*, $M0$ and $M9$ before performing the expensive operations. In this way, it can prevent this attack. On the other hand, ESS-FH uses the digital signature to protect the *RtAdv* message in the initialization phase. If the *MN* is not time-synchronized with the *AR*, it just believes that the *AR* once sent the *RtAdv* message to itself because of not being able to verify that the message is fresh. However, in order to exploit this vulnerability, the adversary should just replay the previous messages since it is so difficult to steal the *AR*'s private key. That is, the adversary cannot freely forge the message. Moreover, the information given in the *RtAdv* message is seldom changed, and the initialization phase happens only during the *MN*'s bootstrapping stage. Thus, such an attack is not effective. As a result, ESS-FH is not vulnerable to the DoS attack which Kang-Park's scheme suffers from.

5. Performance Evaluation

In this section, an analytical model is derived for evaluating ESS-FH compared to Kang-Park's scheme. Then, we present the numerical results where the handover latencies for both schemes are analyzed.

5.1 Analytical Model

5.1.1 Mobility Model

The Markov chain based probabilistic random walk mobility model is used as our mobility model. In this mobility model, the *MN* is assumed to be moving with a particular speed and in a particular direction for a given interval time [12], [13]. Let p be the probability that the *MN* stays within the current MAP domain. Then, $1 - p$ is the probability that the *MN* moves to another MAP domain. The transition probability matrix for the movement probabilities is expressed as:

$$p_{i,j} = \begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix}. \quad (1)$$

Let π_0 and π_1 be the long-term steady state probabilities that an *MN* stays in the current MAP domain and the *MN* moves to another, respectively. Then, π_0 and π_1 are expressed as:

$$\pi_0 = p\pi_0 + (1-p)\pi_1, \quad (2)$$

$$\pi_1 = (1-p)\pi_0 + p\pi_1, \quad (3)$$

where $\pi_0 + \pi_1 = 1$.

5.1.2 Handover Latency Model

The handover latency involving the authentication delay is one of the critical QoS metrics in mobile networks. More precisely, data packets sent to the *MN* will be lost or buffered during the handover. Note that FMIPv6 and F-HMIPv6 which have buffering functionalities prevent the packet loss by applying a buffering technique at *ARs*. In this paper, the L2 handover latency is not considered because the L2 handover latency depends upon the used L2 technologies, *e.g.*, IEEE 802.11 or IEEE 802.16. In MIPv6, the handover latency is defined as the sum of the movement detection delay, address configuration delay, and the registration delay [14], whereas the movement detection delay and the address configuration delay are eliminated by adopting L2 information in FMIPv6 and F-HMIPv6.

In this paper, the following three types of handover latency is modeled: the initial-handover latency for which the *MN* moves from its home work to a new MAP domain, the intra-handover latency for which the *MN* moves from the *AR* to another in the same MAP domain, and the inter-handover latency for which the *MN* moves from the MAP domain to another. The considered scenario is as follows: The *MN* boots up at its home network where the basic MIPv6 functions are supported. Then, it moves to the MAP domain and travels between different *ARs* in the same MAP domain. And the *MN* moves to another MAP domain. For clarity and convenience sake, we suppose that the cryptographic operation and queuing delays at nodes are negligible.

Suppose $L^{(KP)}_{Initial-HO}$ denotes the initial-handover latency of Kang-Park's scheme. It is expressed as:

$$L^{(KP)}_{Initial-HO} = D^{(KP)}_{MD} + D^{(KP)}_{AC} + D^{(KP)}_{Init-REG}, \quad (4)$$

where $D^{(KP)}_{MD}$ is the movement detection delay. As presented in [15], the mean time between unsolicited *RtAdv* messages sent from the *AR* can be expressed as $(MinInt + MaxInt)/2$, where $MinInt$ and $MaxInt$ are the minimum and maximum times allowed between sending unsolicited *RtAdv* messages, respectively, as defined in [1], [16]. $D^{(KP)}_{MD}$ is thus expressed as the half of the mean time between unsolicited *RtAdv* messages:

$$D^{(KP)}_{MD} = \frac{(MinInt + MaxInt)}{4}. \quad (5)$$

In Eq. (4), $D^{(KP)}_{AC}$ is the address configuration delay. The *MN* on receiving the *RtAdv* message generates its address based on the prefix information included in the *RtAdv* message. Then, the *MN* performs the duplicate address detection (DAD) procedure as defined in [1]. Thus, if we assume that the address generation time at the *MN* is negligible, $D^{(KP)}_{AC}$ is expressed as:

$$D^{(KP)}_{AC} = RetransTimer \times DADTransmits, \quad (6)$$

where $RetransTimer$ is the time between retransmissions of *Neighbor Solicitation (NS)* messages defined in [16]. $DADTransmits$ is the number of consecutive *NS* messages sent while performing DAD procedure as defined in [17]. Let t_{MN-AR}, t_{AR-MAP}, t_{MAP-HA}, and $t_{MAP-AAA}$ be the transmission delays between the *MN* and the *AR*, between the *AR* and the *MAP*, between the *MAP* and *HA*, and between the *MAP* and *AAA*, respectively. Then, $D^{(KP)}_{Init-REG}$ shown in Eq. (4) is the registration delay for binding updating to the *HA* and the *MAP* so that can be expressed as:

$$D^{(KP)}_{Init-REG} = max(D^{(KP)}_{REG-HA}, D^{(KP)}_{REG-MAP}), \quad (7)$$

where $D^{(KP)}_{REG-HA}$ is the registration delay to the *HA* and is expressed as $3t_{MN-AR} + 2(t_{AR-MAP} + t_{MAP-HA})$, $D^{(KP)}_{REG-MAP}$ is the registration delay to the *MAG* and is expressed as $3t_{MN-AR} + 2(t_{AR-MAP} + t_{MAP-AAA})$.

Suppose $L^{(ESS-FH)}_{Initial-HO}$ denotes the initial-handover latency of proposed ESS-FH. Similar to Eq. (4), it is expressed as:

$$L^{(ESS-FH)}_{Initial-HO} = D^{(ESS-FH)}_{MD} + D^{(ESS-FH)}_{AC} + D^{(ESS-FH)}_{Init-REG}, \quad (8)$$

where $D^{(ESS-FH)}_{MD}$ and $D^{(ESS-FH)}_{AC}$ are the movement detection delay and address configuration delay of proposed ESS-FH, respectively. Because both Kang-Park's scheme and ESS-FH operate based on F-HMIPv6, $D^{(ESS-FH)}_{MD}$ and $D^{(ESS-FH)}_{AC}$

are obtained by the same ways as presented in Eqs. (5) and (6). In ESS-FH, the SK derivation from the AS depending on the AAA infrastructure which is being used in Kang-Park's scheme does not occur. Thus, $D_{Init-REG}^{(ESS-FH)}$ is expressed as:

$$D_{Init-REG}^{(ESS-FH)} = max(D_{REG-HA}^{(ESS-FH)}, D_{REG-MAP}^{(ESS-FH)}), \quad (9)$$

where $D_{REG-HA}^{(ESS-FH)}$ is the registration delay to the HA and is expressed as $3t_{MN-AR} + 2(t_{AR-MAP} + t_{MAP-HA})$, $D_{REG-MAP}^{(ESS-FH)}$ is the registration delay to the MAG and is expressed as $3t_{MN-AR} + 2t_{AR-MAP}$.

Next, we analyze the intra-handover latency. As mentioned, only the predictive mode is considered†. Let $L_{Intra-HO}^{(KP)}$ denotes the intra-handover latency of Kang-Park's scheme. It is expressed as:

$$L_{Intra-HO}^{(KP)} = 2t_{MN-AR}, \quad (10)$$

where $2t_{MN-AR}$ is the delay for sending the UNA message and receiving the first data packet at the new AR.

Let $L_{Intra-HO}^{(ESS-FH)}$ denotes the intra-handover latency of proposed ESS-FH. It is expressed as:

$$L_{Intra-HO}^{(ESS-FH)} = L_{Intra-HO}^{(KP)}. \quad (11)$$

In ESS-FH, the local binding update is executed by exchanging the LBU and LBA messages between the MN and the MAP after the MN moves to the nAR. However, as the nAR receives the UNA message sent from MN, the buffered data packets are immediately sent to the MN.

Now, the inter-handover latency is analyzed. Let $L_{Inter-HO}^{(PK)}$ denotes the inter-handover latency of Kang-Park's scheme, where the MN performs its inter-handover as the same of MIPv6 or HMIPv6. This is, the fast handover between the different MAP domains cannot be supported. Thus, $L_{Inter-HO}^{(PK)}$ is expressed as:

$$L_{Inter-HO}^{(KP)} = L_{Initial-HO}^{(KP)}. \quad (12)$$

Suppose $L_{Inter-HO}^{(ESS-FH)}$ denotes the inter-handover latency of proposed ESS-FH. As described in Sect. 3.2.3, ESS-FH enables the fast handover between the different MAP domains when the MN performs its inter-handover. Thus, $L_{Inter-HO}^{(ESS-FH)}$ is expressed as:

$$L_{Inter-HO}^{(ESS-FH)} = L_{Intra-HO}^{(ESS-FH)}. \quad (13)$$

5.2 Numerical Results

For our numerical analysis, the following transmission delays are assumed: $t_{MN-AR} = 12$ ms, $t_{AR-MAP} = 20$ ms, $t_{MAP-HA} = t_{MAP-AAA} = 40$ ms. For parameters for nodes, $MinInt$ and $MaxInt$ are set as 30 ms and 70 ms, respectively. $RetransTimer$ and $DADTransmits$ are set as 1000 ms and 1, respectively [15].

Figure 5 presents each type of handover latency. For both of Kang-Park's scheme and proposed ESS-FH, we first observe that when the MN performs its initial-handover to a new MAP domain managed by Kang-Park's scheme or proposed ESS-FH, the initial-handover latencies for them are the same. This is because that the MN moves from the network where the fast handover is not being supported so that neither of them can utilize L2 information for executing the fast handover. For the intra-handover latency, we can see that both of them achieve the reduced handover latency due to the effects of fast handover. The inter-handover latency of Kang-Park's scheme is much larger than that of ESS-FH. This is because that when the MN moves between the different MAP domains, the fast handover to the MN cannot be supported in Kang-Park's scheme.

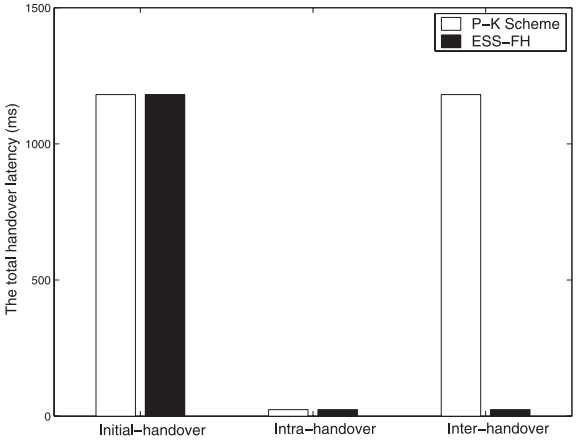

Fig. 5 Each type of handover latency.

The results presented in Fig. 5 provide the fact that ESS-FH outperforms Kang-Park's scheme in terms of the inter-handover latency. In order to investigate more details on the handover latency, we utilize the mobility model presented in Sect. 5.1.1. Then, the handover latency regarding movement probabilities can be expressed as:

$$L_{HO}^{(PK)} = \frac{L_{Intra-HO}^{(PK)}(1-\pi_1) + L_{Inter-HO}^{(PK)}\pi_1}{T}, \quad (14)$$

$$L_{HO}^{(ESS-FH)} = \frac{L_{Intra-HO}^{(ESS-FH)}(1-\pi_1) + L_{Inter-HO}^{(ESS-FH)}\pi_1}{T}, \quad (15)$$

where T is the average resident time of the MN at the MAP domain.

Figure 6 shows the handover latency as a function of T. As we can see in Fig. 6, ESS-FH always outperforms Kang-Park's scheme due to the effect of the fast handover when the MN performs its inter-handover between the different MAP domains. Accordingly, T is not a sensitive performance factor in ESS-FH, whereas Kang-Park's scheme is largely affected by T.

†F-HMIPv6 operates based on the movement prediction information obtained from L2 information and it may be undeterminable. So, adopting the prediction probability P_s is open used in study of FMIPv6 and F-HMIPv6 [18]. However, in this paper, P_s is set as 1 to focus on the performance of the predictive mode.

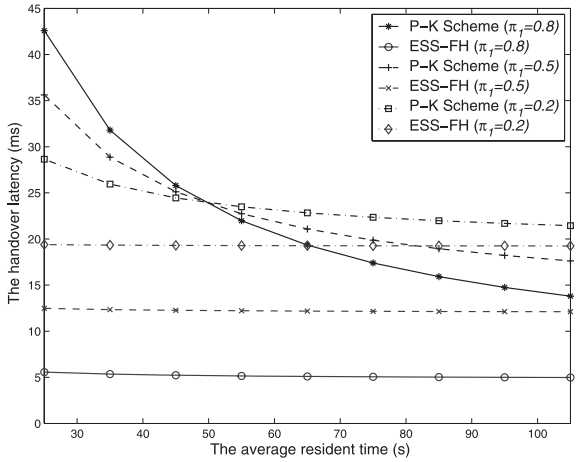

Fig. 6 The handover latency as a function of T.

6. Conclusions

In this paper, we have proposed the Enhanced Security Scheme for Fast Handover in Hierarchical Mobile IPv6, called ESS-FH. ESS-FH makes use of the *CGA* method and the public key cryptography to provide the strong key exchange as well as the key independence. At the same time, it defends against the DoS and redirection attacks, which Kang-Park's scheme suffers from. Moreover, ESS-FH achieves the fast handover even mobile nodes perform the inter-handover between different Hierarchical Mobile IPv6 domains. In order to show its superiority, we performed formal security analysis as well as performance evaluation. According to the results, it is shown that ESS-FH achieves both strong security and good efficiency.

References

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF RFC 3775, June 2004.
[2] R. Koodli, "Mobile IPv6 Fast Handovers," IETF RFC 5268, June 2008.
[3] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier, "Hierarchical mobile IPv6 (HMIPv6) mobility management," IETF RFC 5380, Oct. 2008.
[4] H. Jung, H. Soliman, S. Koh, and J. Lee, "Fast handover for hierarchical MIPv6 (F-HMIPv6)," IETF Internet Draft, draft-jung-mobopts-fhmipv6-00.txt, April 2005.
[5] H. Jung, E. Kim, J. Yi, and H. Lee, "A scheme for supporting fast handover in hierarchical mobile IPv6 networks," ETRI Journal, vol.27, no.6, pp.798–801, Dec. 2005.
[6] S. Fu and M. Atiquzzaman, "Handover latency comparison of SIGMA, FMIPv6, HMIPv6, and FHMIPv6," Proc. IEEE GLOBECOM 2005, vol.6, pp.3809–3813, Dec. 2005.
[7] R.H. Deng, J. Zhou, and F. Bao, "Defending against redirect attacks in mobile IP," Proc. 9th ACM Conference on Computer and Communications Security, pp.59–67, 2002.
[8] H. Kang and C. Park, "Authenticated fast handover scheme in the hierarchical mobile IPv6," Lect. Notes Comput. Sci., vol.4298, pp.211–224, 2007.
[9] T. Aura, "Cryptographically generated addresses (CGA)," IETF RFC 3972, March 2005.
[10] C. Perkins and P. Calhoun, "Authentication, authorization, and accounting (AAA) registration keys for mobile IPv4," IETF RFC 3957, March 2005.
[11] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol.8, no.1, pp.18–36, 1990.
[12] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," Wireless Communications and Mobile Computing, vol.2, no.5, pp.483–502, Sept. 2002.
[13] J.H. Kim, C.S. Hong, and T. Shon, "A lightweight NEMO protocol to support 6LoWPAN," ETRI Journal, vol.30, no.5, pp.685–695, Oct. 2008.
[14] J.-H. Lee, Y.-J. Han, H.-J. Lim, and T.-M. Chung, "New binding update method using GDMHA in hierarchical mobile IPv6," Lect. Notes Comput. Sci., vol.3480, pp.146–155, 2005.
[15] K.-S. Kong, W. Lee, Y.-H. Han, and M.-K. Shin, "Handover latency analysis of a network-based localized mobility management protocol," Proc. IEEE International Conference on Communications (ICC) 2008, pp.5838–5843, May 2008.
[16] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," IETF RFC 2461, Dec. 1998.
[17] S. Thomson and T. Narten, "IPv6 stateless address autoconfiguration," IETF RFC 2462, Dec. 1998.
[18] C. Makaya and S. Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols," IEEE Trans. Wirel. Commun., vol.7, no.3, pp.972–983, March 2008.

Ilsun You received his M.S. and Ph.D. degrees in Computer Science from Dankook University, Seoul, Korea in 1997 and 2002, respectively. Since March 2005, he has been an Assistant Professor in the School of Information Science at the Korean Bible University, South Korea. His main research interests include network security and authentication. He is a member of the KIISC and KSII.

Jong-Hyouk Lee received his B.S. degree in Information System Engineering from Daejeon University, Daejeon, Korea in 2004 and his M.S. degree in Computer Engineering at Sungkyunkwan University, Suwon, Korea in 2007. He obtained his Ph.D. degree in Electrical and Computer Engineering at Sungkyunkwan University in 2010. He worked as an intern for IMARA Team, INRIA, France in 2009. He received Excellent Research Awards (two times) from Department of Electrical and Computer Engineering, Sungkyunkwan University. He received Best Paper Award from International Conference on Systems and Networks Communications 2008. Currently, he is a postdoctoral researcher in IMARA Team, INRIA, France. He is now developing a solution to make efficient and secure communications for NEMO based vehicular networks. His research interests include mobility management, security, and performance analysis based on protocol operation for next-generation wireless mobile networks.

Kouichi Sakurai received B.E., M.E., and D.E. degrees from Kyushu University, Fukuoka, Japan in 1986, 1988, and 1993, respectively. From 1986 to 1993, he was a Researcher of Mitsubishi Electronics Co., Ltd. From 1994 to 2001, he was an Associate Professor in the Department of Computer Science and Communication Engineering, Kyushu University. From 2002, he has been a Professor in the Department of Computer Science and Communication Engineering, Kyushu University. From 2004, he has been also the general manager of information security laboratory of Institute of Systems, Information Technologies (ISIT).

Yoshiaki Hori received B.E., M.E., and D.E. degrees from Kyushu Institute of Technology, Iizuka, Japan in 1992, 1994, and 2002, respectively. From 1994 to 2003, he was a Research Associate in Common Technical Courses, Kyushu Institute of Design, Fukuoka. From 2003 to 2004, he was a Research Associate in the Department of Art and Information Design, Kyushu University, Fukuoka. Since March 2004, he has been an Associate Professor in the Department of Computer Science and Communication Engineering, Kyushu University.