Mobile Information Systems 7 (2011) 271–283
DOI 10.3233/MIS-2011-0121
IOS Press

Enhancing MISP with Fast Mobile IPv6 Security

Ilsun You[a], Jong-Hyouk Lee[b,*], Yoshiaki Hori[c] and Kouichi Sakurai[c]
[a]*Korean Bible University, Seoul, Korea*
[b]*INRIA, Paris, France*
[c]*Kyushu University, Fukuoka, Japan*

Abstract. The Mobile Broadband Association has developed the MIS and MISAUTH protocols as link-layer fast authentication protocols. A combination of MIS and MISAUTH protocols, called as MISP, provides secure and fast connection for a wireless access network, but it has been reported that MISP creates a weak session key and suffers from a denial-of-service attack. In addition, a transaction with an authentication server that is required for every authentication is considered as a delay factor during handovers. In this paper, we present an improvement of MISP that utilizes the fast handover approach of Fast Mobile IPv6 and minimizes an involvement of the authentication server while eliminating identified security drawbacks of MISP. The formal security analysis is performed to verify the correctness of the proposed scheme. Moreover, the handover performance of the proposed scheme is compared with an existing scheme.

Keywords: MISP, FMIPv6, BAN-Logic

1. Introduction

IEEE 802.11, which is a set of standards for a wireless access network, has gained considerable popularity because of many advantages such as convenience, flexibility, easy installation, and low cost [1]. However, IEEE 802.11 incurs long handover latency, especially during access network authentication based on IEEE 802.11i or IEEE 802.1X [2,3] so it is not satisfiable for time-sensitive application such as VoIP [4]. One of efforts to overcome such limitations is a development of MIS and MISAUTH protocols, hereafter we call a combination of MIS and MISAUTH protocols as MISP, from the Mobile Broadband Association (MBA) [5,6]. Note that the MBA develops specifications for Internet mobile broadband services mostly based on Japan. MIS is designed to provide authentication, IP address assignment, session key exchange, and various negotiations between a Mobile Node (*MN*) and a Base Router (*BR*), whereas MISAUTHP is designed to allow the *BR* to authenticate the *MN* with an Authentication Server (*AS*). Since MISP establishes a secure connection between the *MN* and the *BR* in a short time, it has been considered to be an efficient and fast authentication method for a wireless access network in Japan.

However, as reported in [7], MISP has the following security drawbacks: 1) Because the user password is utilized as a secret key, MISP is vulnerable to off-line dictionary attacks; 2) The session key is weak because a *MN* decides its session key at its will; and 3) Denial-of-service attacks are valid because the

*Corresponding author: Jong-Hyouk Lee, IMARA Team, Bt. 07, INRIA Paris - Rocquencourt, Domaine de Voluceau Rocquencourt - B.P. 105, 78153, Le Chesnay Cedex, France. Tel.: +33 1 39 63 59 30; E-mail: jong-hyouk.lee@inria.fr.

1574-017X/11/$27.50 © 2011 – IOS Press and the authors. All rights reserved

Table 1
Used notations

Notation	Description
MN, *BR*, *AS*	mobile node, base router, and authentication server, respectively
secType	security type specifying authentication, session key delivery, and encryption methods
secTypes	list of the security types
H(*M*)	one-way hash value on the message M
HMAC(*K, M*)	HMAC value computed using the key K over the message M
ID_X	identifier of X, where X can be an entity or message
PU_{MN}	public key of *MN*
K_{MN}	secret key shared between *MN* and *AS*
MA_X	MAC (interface) address of X
K_{AB}	secret key shared between *AS* and *BS*
SK	session key shared between *MN* and *BR*
$K(i)$	i-th message protection key, $i > 0$
lt	lifetime of SK
$ts, ts1, ts2, ts3$	timestamp
$\|$	concatenation operation
$\oplus$	exclusive-OR operation

beacon and authentication failure messages are not completely protected during the protocol operation. From the viewpoint of handover performance, a transaction with the *AS* for every authentication increases handover latency. Note that MISP only supports secure link-layer handovers so that the authentication related transaction with the *AS* is occurred whenever the *MN* performs its handover at the link-layer or network-layer.

As user mobility is increased, a network-layer handover is frequently occurred, i.e., a *MN*'s movement from one access network to another access network [8,9]. The network-layer handover causes time-consuming procedures including the movement detection, IP address configuration, and location registration that also consume a significant amount of wireless resources compared to procedures in a link-layer handover. Accordingly, in this paper, we develop an improvement of MISP that further considers secure network-layer handovers. We adopt the fast handover approach of Fast Mobile IPv6 (FMIPv6) [10–12] to improve overall handover performance with MISP, while we develop secure handover authentication for link-layer and network-layer handovers. Note that previous studies [13–16] for secure fast handover have considered only either the link-layer handover or network-layer handover. The proposed scheme employs the idea of cross-layer security architecture that allows to exchange security credentials across different layers, e.g., link-layer and network-layer.

This paper is organized as follows. Section 2 describes the operation procedures of the proposed scheme. Section 3 shows the formal security analysis to verify the correctness of the proposed scheme. Section 4 provides a simple performance comparison of the proposed scheme with the existing scheme. Then, Section 5 concludes this paper.

2. Enhancement

In this section, we introduce an improvement of MISP utilizes the fast handover approach of Fast Mobile IPv6 and minimizes an involvement of the authentication server while eliminating identified security drawbacks of MISP. To protect the messages of FMIPv6, we combine a security scheme for FMIPv6 previously proposed by You, Hori, and Sakurai in [17] with MISP. Note that the security scheme is called as YHSP hereafter.

The proposed scheme is consisted of the bootstrapping and handover phases. When a *MN* is power on or is attached to an access network at the first time, the bootstrapping phase is executed, whereas the handover phase is executed when the *MN* performs its handover from one access network to another access network. In the proposed scheme, YHSP relies on MISP to create the first message protection secret instead of the use of the Authentication, Authorization, and Accounting (AAA) infrastructure [18, 19] during the bootstrapping phase. During the handover phase, a new message protection secret established in YHSP is used to derive a new session key in MISP. In this way, the session key is not weak and not vulnerable to the off-line dictionary attacks. Moreover, the new secret is safely forwarded to the next *BR*, i.e., the next *AR*, via a secure channel established between neighboring *BR*s. That makes it possible for the next *BR* to authenticate the *MN* and its message without the involvement of *AS*. Note that the *BR* serves as both an access point and an access router in MISP. Table 1 shows the used notations in this paper.

The followings are assumptions for the proposed scheme:

- A secure channel between neighboring *BRs* exists. For instance, the neighboring *BRs* share a secret key to establish a secure channel.
- An *AS* centrally manages registered users' account information, i.e., ID_{MN} and K_{MN}.
- A *BR* and an *AS* share a shared secret K_{AB} in advance or they can establish that secret when needed.
- A *BR* and an *AS* are time-synchronized.
- A *MN* has a public/private key pair PU_{MN}/PR_{MN}, and its Care-of Address (CoA) is a Cryptographically Generated Address (CGA), which is derived from PU_{MN} [20,21].

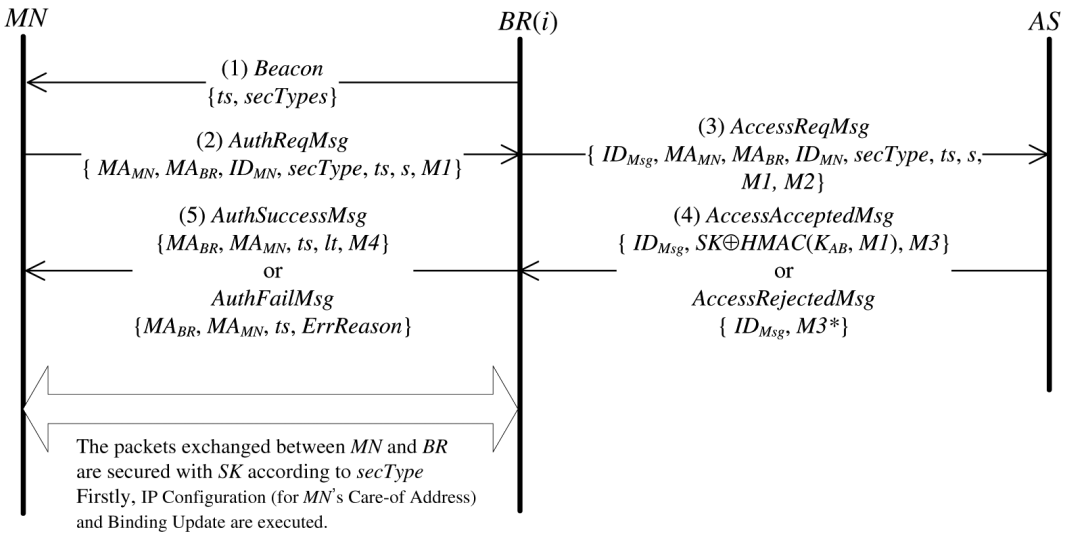
In the following, we describe the bootstrapping and handover phases, separately. Note that we only consider the predictive fast handover mode of FMIPv6 since this mode results in shorter latency than the reactive fast handover mode.

2.1. Bootstrapping phase

Figure 1 shows the bootstrapping phase wherein a *MN* executes the full MISP to establish a secure connection with a *BR*. In order to address the security problems of MISP, MISP is modified as follows: 1) A secret key, K_{MN}, is randomly generated for each user, i.e., *MN*, that is securely registered to the the user's *AS* and mobile device(s), and used for authentication and session key exchange instead of the user password whenever MISP is executed. Such a strong secret key will not cause MISP to be vulnerable to the off-line dictionary attacks; and 2) the session key, *SK*, is computed as follows: $SK = HMAC(K_{MN}, s|ts)$, where s is a value randomly generated by the *MN*. The *MN* cannot generate the session key at its will because the key is derived from the timestamp ts in addition to K_{MN} and s.

As a result of this phase, the *MN* and the *BR* share the session key, *SK*, which will be used later as the first message protection secret, $K(1)$, for the first handover. Also, the phase is followed by the IP address configuration and location registration if needed.

In the bootstrapping phase, we do not consider to protect the beacon and authentication fail messages like the original MISP due to the high cost and complexity. Note that to secure these messages, the *MN* and the *BR* should have a shared secret in advance or should be able to establish a shared secret that clearly makes the bootstrapping phase suffers from the high cost and complexity. Also, the DoS attacks caused by this vulnerability are assumed to be negligible.



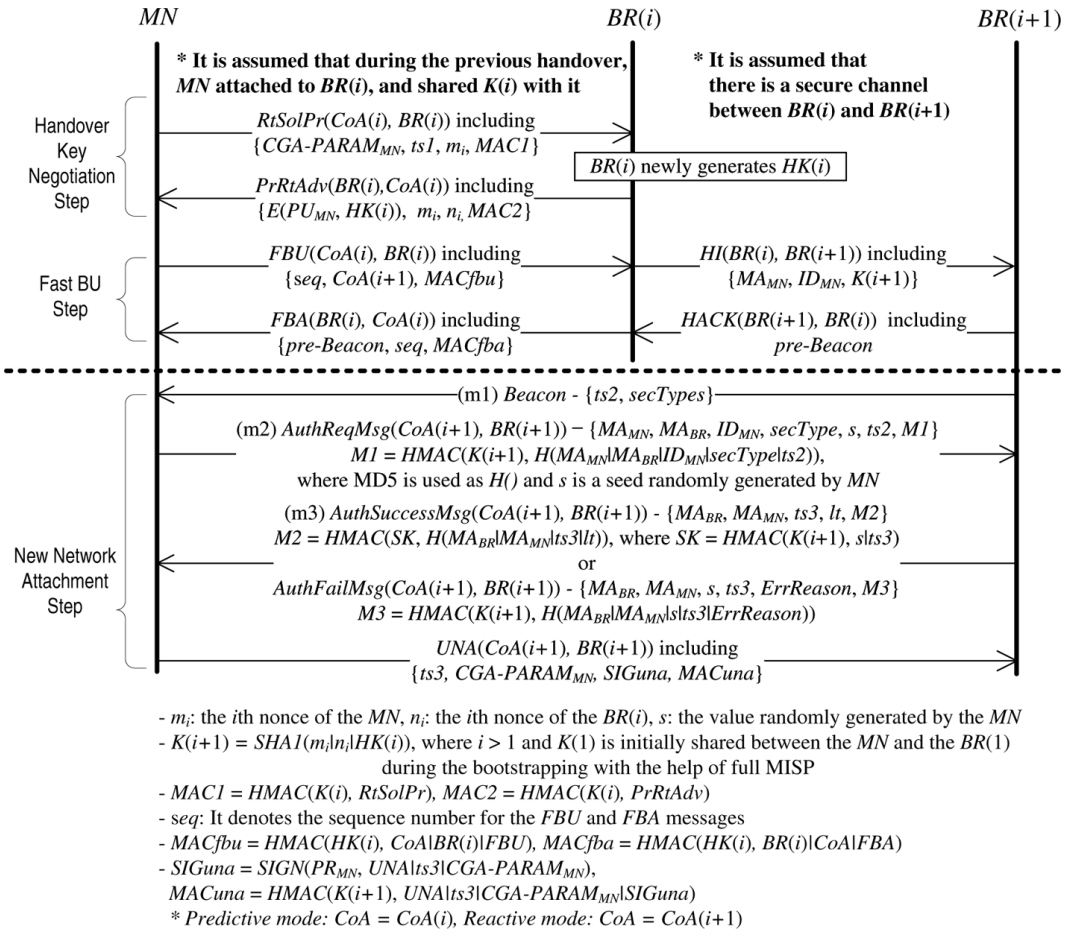
- *secType* has three types as follows: (o: optional, m: mandate)
  1) Null (o), 2) HMAC-MD5/HMAC-MD5/AES-CBC-128bit (m), 3) HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit (o)
  For example, if the 2) type is selected, the used algorithm is as follows:
  (i) authentication:HMAC-MD5, (ii) session key delivery: HMAC-MD5, (iii) encryption: AES-CBC-128
- *ts*: timestamp, ID_{Msg}: the message identifier
- $SK = HMAC(K_{MN}, s|ts)$, where *s* is a seed randomly generated by *MN*
- $M1 = HMAC(K_{MN}, H(MA_{MN}|MA_{BR}|ID_{MN}|secType|ts|s))$, where MD5 is used as *H()*
- $M2 = HMAC(K_{AB}, MA_{MN}|MA_{BR}|ID_{MN}|secType|ts|s|M1)$
- $M3 = HMAC(K_{AB}, ID_{Msg}|SK \oplus HMAC(K_{AB}, M1))$, $M3^* = HMAC(K_{AB}, ID_{Msg})$
- $M4 = HMAC(SK, H(MA_{BR}|MA_{MN}|ts|lt))$
- *ErrReason*: the reason why the authentication fails

Fig. 1. Bootstrapping phase.

2.2. Handover phase

In this subsection, we describe the handover phase composed of the three steps: handover key negotiation, fast binding update, and new network attachment steps. The first two steps, i.e., handover key negotiation and fast binding update steps, are protected by utilizing YHSP and the last step, i.e., new network attachment step, is protected by utilizing MISP.

Figure 2 shows the handover phase. The handover key negotiation step is started as the *MN* recognizes its movement. When the layer-2 triggers indicate the movement, the *MN* performs this step by exchanging the Router Solicitation for Proxy Advertisement (*RtSolPr*) and Proxy Router Advertisement (*PrRtAdv*) messages with the current base router, $BR(i)$. These messages are protected by the message protection key, $K(i)$, which was established in the previous handover or in the bootstrapping phase. After verifying the *PrRtAdv* message, the *MN* configures its new CoA, $CoA(i+1)$. At the same time, it recovers the new handover key, $HK(i)$, by decrypting $E(PU_{MN}, HK(i))$ with its private key. Then, it derives the new message protection key, $K(i+1)$. Note that $K(i+1)$ will be used to protect the *AuthReqMsg* and *AuthFailMsg* messages and to exchange the new session key, SK, in the new network attachment step later. In other words, the network-layer handover security credential, i.e., $K(i+1)$, is used during the link-layer handover. It is worth to note that while the $BR(i)$ verifies PU_{MN} with $CGAP_{MN}$ to prevent the man-in-the-middle attack prior to using that public key, the *MN* firstly verifies *MAC1* to prevent the DoS attacks before the public key decryption.



- m_i: the ith nonce of the *MN*, n_i: the ith nonce of the *BR*(i), s: the value randomly generated by the *MN*
- $K(i+1) = SHA1(m_i|n_i|HK(i))$, where $i > 1$ and $K(1)$ is initially shared between the *MN* and the *BR*(1) during the bootstrapping with the help of full MISP
- *MAC1* = *HMAC*(*K*(*i*), *RtSolPr*), *MAC2* = *HMAC*(*K*(*i*), *PrRtAdv*)
- *seq*: It denotes the sequence number for the *FBU* and *FBA* messages
- *MACfbu* = *HMAC*(*HK*(*i*), *CoA*|*BR*(*i*)|*FBU*), *MACfba* = *HMAC*(*HK*(*i*), *BR*(*i*)|*CoA*|*FBA*)
- *SIGuna* = *SIGN*(PR_{MN}, *UNA*|*ts3*|*CGA-PARAM*$_{MN}$), *MACuna* = *HMAC*(*K*(*i*+1), *UNA*|*ts3*|*CGA-PARAM*$_{MN}$|*SIGuna*)
- * *Predictive mode: CoA* = *CoA*(*i*), *Reactive mode: CoA* = *CoA*(*i*+1)

Fig. 2. Handover phase.

Once $HK(i)$ is established and $CoA(i+1)$ is configured, the *MN* starts to perform the fast binding update step by sending the Fast Binding Update (*FBU*) message to the $BR(i+1)$. If *MACfbu* is valid, the $BR(i+1)$ believes that the *MN* indeed owns $CoA(i)$ and it is associated with $CoA(i+1)$. Based on this belief, by exchanging the Handover Initiate (*HI*) and Handover Acknowledge (*HACK*) messages with the $BR(i+1)$, it informs the $BR(i+1)$ of $CoA(i+1)$ and $K(i+1)$, and establishes a tunnel between the $BR(i+1)$ and itself to forward the traffic sent from $CoA(i)$ to $CoA(i+1)$. Also, it starts to serve as a temporary Home Agent (*HA*) for the *MN* [10]. Based on $K(i+1)$, the $BR(i+1)$ can authenticate the *MN* and its messages without the *AS*. That makes it possible to considerably reduce handover latency while excluding the *AS* in authentication. Note that there is a secure channel between the $BR(i)$ and the $BR(i+1)$ and this channel is used to protect the above operations. In addition, to defend against the malicious beacon messages, the $BR(i+1)$ adds the *Pre-Beacon* including its current beacon information to the *HACK* one. Finally, the $BR(i)$ concludes this step by returning the *Fast Binding Acknowledge* (*FBA*) message to the *MN*.

When the *MN* attaches to the new network, it receives the beacon messages from multiple *BRs*. With the *Pre-Beacon*, it finds the valid beacon message and the $BR(i+1)$, then preparing for the *AuthReqMsg* message after selecting the proper security type *secType*. Upon receiving the *AuthReqMsg* message, the

$P \equiv X$	*P believes X*
$P \triangleleft X$	*P sees X*
$P \mid\sim X$	*P once said X*
$P \Rightarrow X$	*P has jurisdiction over X*
$\#(X)$	*X* is *fresh*
$P \overset{K}{\leftrightarrow} Q$	*P* and *Q* may use the shred *key K* to communicate
$\{X\}_K$	*X* is encrypted under the key *X*
$+\{M\}_K$	$= (M, \{H(M)\}_K)$ where $H(\cdot)$ denotes one way hash function

Fig. 3. Notations of BAN-Logic.

R1: Message-Meaning Rule

$$\frac{P \equiv P \overset{K}{\leftrightarrow} Q,\ P \triangleleft \{X\}_K}{P \equiv Q \mid\sim X}$$

R2: Nonce-Verification Rule

$$\frac{P \equiv \#(X),\ P \equiv Q \mid\sim X}{P \equiv Q \equiv X}$$

R3: Jurisdiction Rule

$$\frac{P \equiv Q \Rightarrow X,\ P \equiv Q \equiv X}{P \equiv X}$$

R4: Hash Rule

$$\frac{P \equiv Q \mid\sim H(X),\ P \triangleleft X}{P \equiv Q \mid\sim X}$$

R5: Other Rules

$$\frac{P \equiv \#(X)}{P \equiv \#(X, Y)} \qquad \frac{P \equiv (X, Y)}{P \equiv X} \qquad \frac{P \equiv \overset{K}{\mapsto} P,\ \ P \triangleleft \{X\}_K}{P \triangleleft X}$$

Fig. 4. Rules of BAN-logic

$BR(i+1)$ verifies *M1* with $K(i+1)$ and checks if the included *ts2* and *secType* are acceptable. If the verification is positive, it has the belief on the *MN*, based on which it derives the session key, *SK*, by computing $HMAC(K(i+1), s|ts3)$. Then, the $BR(i+1)$ sends the *MN* the *AuthSuccessMsg* message protected with *SK*, which is not weak and vulnerable to the off-line dictionary attacks any more. If the message is valid, the *MN* is sure that it is safely connected to the $BR(i+1)$. Finally, the *MN* sends the $BR(i+1)$ the *Unsolicited Neighbor Advertisement* (*UNA*) message protected with *SIGuna* and *MACuna*. Here, *MACuna* allows the $BR(i+1)$ to defend against the resource exhaustion attacks caused by abuse of the digital signatures. If the *AuthReqMsg* message is not valid, i.e., it cannot be verified with $K(i+1)$, the $BR(i+1)$ responds with the *AuthFailMsg* message. Because the message is protected with $K(i+1)$, it does not cause MISP to be vulnerable to the DoS attacks.

3. Security analysis

In this section, we formally verify the correctness of the proposed scheme by using BAN-Logic [22]. BAN-Logic has been widely used and successfully applied to analyze many security schemes (protocols) because it is simple, easy, and practical [22–24].

In BAN-Logic, the security verification consists of the following steps: 1) Translate a target protocol into an idealization version; 2) Define assumptions about the initial states; and 3) Apply repeatedly the rules until the intended beliefs are derived. The notations and rules of BAN-logic are shown in Figs 3 and 4. Note that we use $H(M)_K$ to express the HMAC operation since original BAN-Logic does not support [25].

E1: Extended Rule1

$$\frac{P \equiv P \overset{K}{\leftrightarrow} Q,\ P \triangleleft +\{H(M)\}_K}{P \equiv Q \sim M}$$

E2: Extended Rule2

$$\frac{P \equiv \overset{K}{\mapsto} P,\quad P \equiv \{X\}_K}{P \equiv X}$$

Fig. 5. Extended rules of BAN-logic.

In order to make the verification more concise and convenient, the extended rules are defined as depicted in Fig. 5. E1 can be proofed by using the rules R1 and R4, while E2 is self-evident.

For the formal analysis on the proposed scheme, while focusing on the handover phase, we first verify the handover key negotiation and fast binding update steps, protected by YHSP, and then verify the new network attachment one, protected by MISP. That is why its new network attachment step is same as the bootstrapping phase if we ignore that the beacon and *AuthFailMsg* messages are unsecured in that phase. Such neglect is acceptable because of the complexity and the high cost caused by protecting these messages in the bootstrapping phase as mentioned above.

3.1. Handover key negotiation and fast binding update steps

As the first step, we idealize the handover key negotiation and fast binding update steps as follows:

(yhsp1) $MN \rightarrow BR(i) : +\{RtSolPr\}_{K(i)}$
where *RtSolPr* includes $\{CGA\text{-}PARAM_{MN}, ts1, mi\}$
(yhsp2) $BR(i) \rightarrow MN: +\{PrRtAdv\}_{K(i)}$
where *PrRtAdv* includes $\{\{MN \overset{HK(i)}{\leftrightarrow} BR(i), MN \overset{K(i+1)}{\leftrightarrow} BR(i)\}_{PU_{MN}},\ mi, ni\}$
(yhsp3) $MN \rightarrow BR(i) : +\{FBU\}_{HK(i)}$
where *FBU* includes $\{seq, MN \equiv MN \overset{HK(i)}{\leftrightarrow} BR(i), MN \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i), CoA(i{+}1)\}$
(yhsp4) $BR(i) \rightarrow MN : +\{FBA\}_{HK(i)}$
where *FBA* includes $\{seq, pre\text{-}Beacon\}$

We here skip the *HI* and *HACK* messages in the idealized form because they are transmitted over the secure channel between the $BR(i)$ and the $BR(i+1)$.

The assumptions are defined as follows:

A11: $BR(i) \equiv BR(i) \overset{K(i)}{\leftrightarrow} MN$
A12: $BR(i) \equiv \#(ts1)$
A13: $MN \equiv BR(i) \overset{K(i)}{\leftrightarrow} MN$
A14: $MN \equiv \#(mi)$
A15: $MN \equiv \overset{PU_{MN}}{\mapsto} MN$
A16: $MN \equiv BR(i) \Rightarrow BR(i) \overset{HK(i)}{\leftrightarrow} MN$
A17: $MN \equiv BR(i) \Rightarrow BR(i) \overset{K(i+1)}{\leftrightarrow} MN$
A18: $BR(i) \equiv MN \overset{HK(i)}{\leftrightarrow} BR(i)$
A19: $BR(i) \equiv \#(MN \overset{HK(i)}{\leftrightarrow} BR(i))$
A1a: $BR(i) \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i)$
A1b: $BR(i) \equiv \#(MN \overset{K(i+1)}{\leftrightarrow} BR(i))$
A1c: $BR(i) \equiv MN \Rightarrow MN \equiv MN \overset{HK(i)}{\leftrightarrow} BR(i)$
A1d: $BR(i) \equiv MN \Rightarrow MN \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i)$
A1e: $MN \equiv \#(seq)$

In the above assumptions, A11 and A13 are added because the message protection key, $K(i)$, is assumed to be shared between the *MN* and the $BR(i)$ in the previous handover. In addition, it is acceptable to add A1c and A1d as an entity is generally authorized to believe its session keys.

With the idealized form and the assumptions, we proceed to verify the handover key negotiation and fast binding update steps as follows:

From yhsp1, we derive:
(1a) $BR(i) \equiv MN \mid\sim RtSolPr$ [by A11, E1]
(1b) $BR(i) \equiv \#(RtSolPr)$ [by A12, R5]
(1c) $BR(i) \equiv MN \equiv RtSolPr$ [by (1a), (1b), R2]

From yhsp2, we derive:
(1d) $MN \equiv BR(i) \mid\sim PrRtAdv$ [by A13, E1]
(1e) $MN \equiv \#(PrRtAdv)$ [by A14, R5]
(1f) $MN \equiv BR(i) \equiv PrRtAdv$ [by 1d, 1e, R2]
(1g) $MN \equiv MN \overset{HK(i)}{\leftrightarrow} BR(i)$ [by 1f, R5, A15, E2, R5, A16, R3]
(1h) $MN \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i)$ [by 1f, R5, A15, E2, R5, A17, R3]

From yhsp3, we derive:
(1i) $BR(i) \equiv MN \equiv FBU$ [by A18, E1, A19, R5, R2]
(1j) $BR(i) \equiv MN \equiv MN \overset{HK(i)}{\leftrightarrow} BR(i)$ [by 1j, R5, A1c, R3]
(1k) $BR(i) \equiv MN \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i)$ [by 1i, R5, A1d, R3]
(1l) $BR(i) \equiv MN \equiv CoA(i)$ [by 1i, R5]

From yhsp4, we derive:
(1m) $MN \equiv BR(i) \equiv FBA$ [by 1g, E1, A1e, R5, R2]
(1n) $MN \equiv BR(i) \equiv pre\text{-}Beacon$ [by 1m, R5]

While (1i) and (1l) allow the $BR(i)$ to believe the handover and the new CoA of the *MN*, (1m) allows the *MN* to believe that the $BR(i)$ accepts its handover. Additionally, through (1g), (1h), (1k) and (1l), the *MN* and the $BR(i)$ can believe that $HK(i)$ and $K(i+1)$ are securely established. That also makes them believe that $K(i+1)$ is safely forwarded to the $BR(i+1)$ for the next handover. Moreover, through the *Pre-Beacon* and (1n), the *MN* can distinguish the beacon message of the $BR(i+1)$ with other ones while defending against the *DoS* attacks.

As a result, we can conclude that the handover key negotiation and fast binding update steps are valid in terms of security.

3.2. New network attachment step

We start the analysis by translating the new network attachment step into the idealized form shown below. In the idealized form, the *Beacon* message is omitted because it is not related to this analysis.

(misp1) $MN \rightarrow BR(i{+}1) : +\{AuthReqMsg\}_{K(i+1)}$
where *AuthReqMsg* includes $\{ts2, MN \overset{SK}{\leftrightarrow} BR(i{+}1)\}$
(misp2a) $BR(i{+}1) \rightarrow MN: +\{AuthSuccessMsg\}_{SK}$
where *AuthSuccessMsg* includes $\{ts3,\ BR(i{+}1) \equiv MN \overset{SK}{\leftrightarrow} BR(i{+}1)\}$
(misp2b) $BR(i{+}1) \rightarrow MN: +\{AuthFailMsg\}_{K(i+1)}$
where *AuthFailMsg* includes $\{ts3, ErrReason\}$
(misp3) $MN \rightarrow BR(i{+}1) : +\{UNA, \{H(UNA)\}_{PR_{MN}}\}_{K(i+1)}$
where *UNA* includes $\{ts3, CGA\text{-}PARAM_{MN}\}$

We define the assumptions as follows:

A21: $BR(i{+}1) \equiv BR(i{+}1) \overset{K(i+1)}{\leftrightarrow} MN$
A22: $BR(i{+}1) \equiv \#(ts2)$
A23: $BR(i{+}1) \equiv MN \Rightarrow BR(i{+}1) \overset{K(i+1)}{\leftrightarrow} MN$
A24: $MN \equiv MN \overset{SK}{\leftrightarrow} BR(i{+}1)$
A25: $MN \equiv MN \overset{K(i+1)}{\leftrightarrow} BR(i{+}1)$
A26: $MN \equiv \#(ts3)$
A27: $MN \equiv BR(i{+}1) \Rightarrow BR(i{+}1) \equiv MN \overset{SK}{\leftrightarrow} BR(i{+}1)$
A28: $MN \equiv BR(i{+}1) \Rightarrow ErrReason$
A29: $BR(i) \equiv \#(ts3)$
A2a: $BR(i) \equiv \overset{PU_{MN}}{\mapsto} MN$

A21 is added to the assumptions because $K(i+1)$ was securely forwarded to the $BR(i+1)$ in the previous step. With regard to A23, it is reasonable for the $BR(i+1)$ to trust the *MN*'s authorization on *SK* since the *MN* cannot decide *SK* at its will in spite of being able to generate the key. Moreover, based on the CGA method, the $BR(i+1)$ can check the *MN*'s public key. Thus, A2a is involved in the assumptions.

With the above idealized form and the assumptions, we advance our verification as follows:

From misp1, we derive:
(2a) $BR(i{+}1) \equiv MN \equiv AuthReqMsg$ [by A21, E1, A22, R5, R2]
(2b) $BR(i{+}1) \equiv MN \overset{SK}{\leftrightarrow} BR(i{+}1)$ [by 2a, R5, A23, R3]

From misp2a, we derive:
(2c1) $MN \equiv BR(i{+}1) \equiv AuthSuccessMsg$ [by A24, E1, A26, R5, R2]
(2c2) $MN \equiv BR(i{+}1) \equiv MN \overset{SK}{\leftrightarrow} BR(i{+}1)$ [by 2c1, R5, A27, R2]

From misp2b, we derive:
(2d1) $MN \equiv BR(i{+}1) \equiv AuthFailMsg$ [by A25, E1, A26, R5, R2]
(2d2) $MN \equiv ErrReason$ [by 2d1, R5, A28, R3]

From misp3, we derive:
(2e) $BR(i{+}1) \equiv MN \equiv \{UNA, \{H(UNA)\}_{PR_{MN}}\}$ [by A21, E1, A29, R5, R2]
(2f) $BR(i{+}1) \equiv MN \equiv UNA$ [by 2e, R5]
(2g) $BR(i{+}1) \equiv MN \equiv UNA$ [by 2e, R5, A2a, E1, R4, A29, R5, R2]

In misp1, the $BR(i+1)$ can authenticate the *MN* through (2a). Also, the *MN* and the $BR(i+1)$ are sure of the trust on *SK* based on (2a), (2b), (2c2) and A24. This indicates that *SK* is not weak any more. In misp2a, (2c1) allows the *MN* to believe that it is successfully authenticated. That triggers the *MN* to send the *UNA* message to advance the rest steps. On the other hand, in case that the authentication is fail, i.e., misp2b, the *MN* can prevent the DoS attacks caused by the message modification or fabrication through (2d1) and (2d2). In misp3, (2f) and (2g) enable the $BR(i+1)$ to be sure that the *MN* arrives at its network. At this point, (2f) allows the $BR(i+1)$ to check if it is reasonable to perform the digital signature verification. That makes it possible for the $BR(i+1)$ to prevent the DoS attacks caused by the large packets.

As a result, from the above analysis, we can conclude that the new network attachment step is correct.

3.3. Discussion

We discuss here how the proposed scheme solves the identified security drawbacks of MISP.

– Session key and Off-line dictionary attacks: In the bootstrapping and handover phases, the timestamp *ts*, *ts2* and *ts3* are used to generate the session key, *SK*. That makes it impossible for every *MN* to make *SK* at its will. Additionally, unlike the original MISP, the randomly generated secrets K_{MN} and $K(i+1)$, instead of the user password, are used for user authentication, message protection and session key establishment. Therefore, the proposed protocol is not vulnerable to the off-line dictionary attacks while providing strong session keys.
– Denial of Service attacks: The *Pre-Beacon* allows the *MN* to check the validity of the beacon message from the *BR*$(i+1)$. Also, the *AuthFailMsg* message is protected with $K(i+1)$. The proposed protocol can thus prevent the adversaries from launching the DoS attacks by maliciously modifying or spoofing these messages.

4. Handover performance

In this section, we evaluate the handover performance of the proposed scheme compared to the basic scheme.

4.1. Analysis of handover latency

We assume that the processing and queuing delays at each entity are negligible and messages over wired/wireless links are transmitted without errors. For the sake of simplicity, we calculate the handover latency as the sum of related message transmission delays over links [16,26]. Suppose $T_{MN\text{-}BR}$ and $T_{BR\text{-}AS}$ are the message transmission delays between the *MN* and the *BR*, and between the *BR* and the *AS*, respectively. Note that $T_{BR\text{-}AS}$ is determined depending on the network topology configuration and $T_{BR\text{-}AS} > T_{MN\text{-}BR}$.

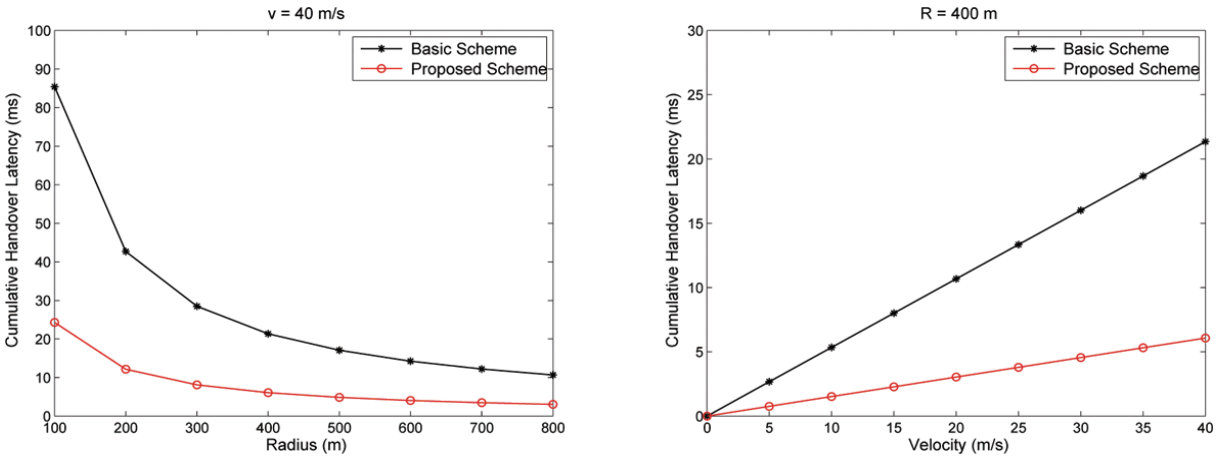
As shown in Fig. 2, the *Beacon*, *AuthReqMsg*, *AuthSuccessMsg*, and *UNA* messages are exchanged between the *MN* and the *BR* at the new access network when the *MN* moves to the new access network. For the basic scheme, IEEE 802.11i fourway handshake, EAP authentication, and *UNA* messages are exchanged. Note that IEEE 802.11i fourway handshake and *UNA* messages are exchanged between the *MN* and the *BR* at the new access network, but EAP authentication messages are exchanged between the *MN* and the *AS*.

Suppose $L_{HO}^{(BASIC)}$ is the handover latency for the basic scheme wherein IEEE 802.11i and 802.1X (EAP-based authentication) are used for authentication while the predictive fast handover mode of FMIPv6 is used for the network-layer mobility support [16]. Then, $L_{HO}^{(BASIC)}$ is expressed as:

$$\begin{aligned} L_{HO}^{(BASIC)} &= D_{L2} + D_{EAP} + D_{SA} + D_{UNA} + D_{FWD}, \\ &= D_{L2} + 9 \cdot T_{MN\text{-}BR} + T_{BR\text{-}AS} + \partial(m,x), \end{aligned} \tag{1}$$

where D_{L2} is the link switching time, i.e., the link-layer handover time, D_{EAP} is the delay of EAP authentication that depends on the selected EAP authentication method, D_{SA} is the delay of IEEE 802.11i fourway handshake, D_{UNA} is the arrival delay of *UNA* message from the *MN* to the *BR*, and D_{FWD} is the arrival delay of the first packet buffered from the *BR* to the *MN*.

In Eq. (1), $9 \cdot T_{MN\text{-}BR}$ represents the time to complete two EAP starting messages (EAP-Request/Identity and EAP-Response/Identity messages), EAP finish message (EAP-Success message), and IEEE 802.11 fourway handshake messages as well as the *UNA* message and the first packet buffered from the *BR* to the *MN*. $T_{BR\text{-}AS}$ represents the delay for forwarding the EAP-Request/Identity message from the *BR*



(a) $L_{HO}^{(\cdot)}$ versus R (b) $L_{HO}^{(\cdot)}$ versus ν

Fig. 6. Cumulative handover latency.

to the *AS*. Since D_{EAP} is determined by the selected EAP authentication method, we adopt a function for calculating the EAP authentication delay $\partial(m, x)$, where m is the number of messages required for executing of the EAP authentication method and x is the message transmission delay between the *MN* and the *AS*, i.e., $x = (T_{MN\text{-}BR} + T_{BR\text{-}AS})$.

Suppose $L_{HO}^{(PRO)}$ is the handover latency for the proposed scheme. Then, $L_{HO}^{(PRO)}$ is expressed as:

$$\begin{aligned} L_{HO}^{(PRO)} &= D_{L2} + D_{Beacon} + D_{AuthReqMsg} + D_{AuthSuccessMsg} + D_{UNA} + D_{FWD}, \\ &= D_{L2} + 5 \cdot T_{MN\text{-}BR}, \end{aligned} \tag{2}$$

where D_{Beacon} is the arrival delay of *Beacon* message from the *BR* to the *MN*, $D_{AuthReqMsg}$ is the arrival delay of *AuthReqMsg* message from the *MN* to the *BR*, and $D_{AuthSuccessMsg}$ is the arrival delay of *AuthSuccessMsg* message from the *BR* to the *MN*.

4.2. Numerical result

In this subsection, we provide the numerical result based on the analysis derived in the previous subsection. For our analysis, we assume that $D_{L2} = 45.35$ ms, $T_{MN\text{-}BR} = 10$ ms, and $T_{BR\text{-}AS} = 20$ ms. If we consider EAP-TLS as the EAP authentication method, m is determined as 6 [14,16].

Let μ_c is the *MN*'s border crossing rate. Assuming that the *BR*'s coverage area is circular, μ_c is expressed as:

$$\mu_c = \frac{2\nu}{\pi R}, \tag{3}$$

where ν is the average velocity of the *MN* and R is the radius of the *BR*'s coverage area [14].

Figure 6 shows the variation of the handover latency. As functions for the variation, we use R and ν. First, we set $\nu = 40$ m/s and vary R from 100 m to 800 m in Fig. 6 (a). As shown, the proposed scheme always provides the minimized handover latency compared to the basic one because of its reduced number of message exchange during handover authentication. In addition, thanks to the elimination of

the *AS*'s involvement during handover authentication, the proposed scheme further improves its handover performance. In Fig. 6 (b), we set $R = 400$ m and vary nu from 0 m/s to 40 m/s. Similarly, the proposed scheme outperforms the basic one.

5. Conclusions

In this paper, we have proposed a secure fast handover scheme that combines advantages of MISP and FMIPv6. We have shown that the proposed scheme is robust against session key, off-line dictionary, DoS attacks while it provides the reduced handover latency compared to the existing scheme. The security correctness of the proposed scheme has been verified through the formal security analysis with BAN-Logic. The proposed scheme is based on FMIPv6, which is a host-based mobility support protocol. The recent approach for mobility support is network-based mobility support wherein a *MN* is not involved in any mobility signaling [27,28]. Our future work is to study our scheme's applicability to network-based mobility support.

References

[1] IEEE Standard 802.11, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
[2] IEEE Standard 802.11i, Security Enhancements, Amendment 6 to IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2004.
[3] IEEE Standard 802.1X, Port-Based Network Access Control, 2001.
[4] H. Morioka, H. Mano, M. Ohmori, C. Jogakuen and M. Ohta, MIS Protocol for Secure Connection and Fast Handover on Wireless LAN, In *Proc of the 20th International Conference on Advanced Information Networking and Applications* (*AINA 2006*) (2006), 533–540.
[5] Mobile Broadband Association, MIS Protocol (MISP) Specification Ver. 1.02, *MBA Standard 0201* (2004).
[6] Mobile Broadband Association, MISAUTH Protocol Specifications Ver. 1.02, *MBA Standard 0301* (2004).
[7] I. You, Y. Hori and K. Sakurai, Toward Formal Analysis of Wireless LAN Security with MIS Protocol, *International Journal of Ad Hoc and Ubiquitous Computing* **7**(2) (2010), 112–120.
[8] A.M. Hanashi, I. Awan and M. Woodward, Performance evaluation with different mobility models for dynamic probabilistic flooding in MANETs, *Mobile Information Systems* **5**(1) (2009), 65–80.
[9] A. Gaddah and T. Kunz, Extending mobility to publish/subscribe systems using a pro-active caching approach, *Mobile Information Systems* **6**(4) (2010), 293–324.
[10] R. Koodli, Mobile IPv6 Fast Handovers, *RFC 5268* (2008).
[11] K. Fujikawa, H. Nakano, M. Ohta, M. Hirabaru, H. Mano and K. Ikeda, A Fast Authentication System for Secure Wireless Internet Services, *IPSJ Technical Report, 2001-DPS-107* (*in Japanese*) (2002).
[12] H. Morioka, Fast Handover with Wireless LAN, *IPSJ Magazine* **45**(8) (2004), 817–820.
[13] A. Durresi, M. Durresi and L. Barolli, Secure Authentication in Heterogeneous Wireless Networks, *Mobile Information Systems* **4**(2) (2008), 119–130.
[14] H. Kim and J.-H. Lee, Diffie-Hellman Key based Authentication in Proxy Mobile IPv6, *Mobile Information Systems* **6**(1) (2010), 107–121.
[15] M. Safar, H. Sawwan, M. Taha and T. Al-Fadhli, Virtual social networks online and mobile systems, *Mobile Information Systems* **5**(3) (2009), 205–311.
[16] J.-H. Lee and T.-M. Chung, Secure Handover for Proxy Mobile IPv6 in Next-Generation Communications: Scenarios and Performance, *Wireless Communications and Mobile Computing* **11**(2) (2011), 176–186.
[17] I. You, K. Sakurai and Y. Hori, An Enhanced Security Protocol for Fast Mobile IPv6, *IEICE Transaction on Information & Systems* **4E92-D**(10) (2009), 1979–1982.
[18] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht and D. Spence, Generic AAA Architecture, *RFC 2903* (2000).
[19] C. Perkins and P. Calhoun, Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, *RFC 3957* (2005).

[20] G. O'Shea and M. Roe, Child-proof authentication for MIPv6 (CAM), *ACM Computer Communications Review* **31**(2) (2001), 4–8.
[21] T. Aura, Cryptographically Generated Addresses (CGA), *RFC 3972* (2005).
[22] M. Burrows, M. Abadi and R. Needham, A Logic of Authentication, *ACM Transaction on Computer Systems* **8**(1) (1990), 18–36.
[23] P. Syverson and I. Cervesato, The Logic of Authentication Protocols, *Lecture Notes In Computer Science* **2171** (2000), 63–136.
[24] C. Meadows, Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends, *IEEE Journal on Selected Areas in Communications* **21**(1) (2003), 44–54.
[25] D. Trcek, MAC Based Lightweight Protocols for Strong Authentication and Key Exchange, *Journal of Information Science and Engineering* **21**(4) (2005), 753–765.
[26] J.-H. Lee and T. Ernst, Fast PMIPv6 Multicast Handover Procedure for Mobility-Unaware Mobile Nodes, In *Proc of IEEE 73rd Vehicular Technology Conference* (*VTC*) *Spring* (2011).
[27] C.J. Bernardos, M. Gramaglia, L.M. Contreras, M. Calderon and I. Soto, Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (*JoWUA*) **1**(2/3) (2010), 16–35.
[28] Z. Yan, H. Zhou and I. You, N-NEMO: A Comprehensive Network Mobility Solution in Proxy Mobile IPv6 Network, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (*JoWUA*) **1**(2/3) (2010), 52–70.

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 IEICE, KIISC and KSII.

Jong-Hyouk Lee received his Ph.D. degree from Sungkyunkwan University, Republic of Korea. He twice received Excellent Research Awards from Department of Electrical and Computer Engineering, Sungkyunkwan University. He is developing efficient secure communications for NEMO based vehicular networks in the project-team IMARA, INRIA, France. He is currently involved in standardization activities at ISO TC204 WG16 (ISO 16788: IPv6 Networking Optimisation and ISO 16789: IPv6 Networking Security) and ETSI TC ITS. His research interests include mobility management, security, and performance analysis based on protocol operations for next-generation wireless mobile networks.

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.

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).