Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 708064, 11 pages
http://dx.doi.org/10.1155/2015/708064

Research Article

A Cross-Layer Key Management Scheme for MIPv6 Fast Handover over IEEE 802.11 Wireless LAN

Chang-Seop Park,[1] Hyun-Sun Kang,[2] and Jaijin Jung[3]

[1]*Department of Software, Dankook University, Jukjeon 16980, Republic of Korea*
[2]*Department of General Education, Namseoul University, Cheonan 31020, Republic of Korea*
[3]*Department of Applied Computer Engineering, Dankook University, Jukjeon 16980, Republic of Korea*

Correspondence should be addressed to Chang-Seop Park; csp0@dankook.ac.kr

Received 21 June 2015; Accepted 29 October 2015

Academic Editor: Francesco Gringoli

A new key management and security scheme is proposed to integrate Layer Two (L2) and Layer Three (L3) keys for secure and fast Mobile IPv6 handover over IEEE 802.11 Wireless Local Area Network (WLAN). Unlike the original IEEE 802.11-based Mobile IPv6 Fast Handover (FMIPv6) that requires time-consuming IEEE 802.1x-based Extensible Authentication Protocol (EAP) authentication on each L3 handover, the newly proposed key management and security scheme requires only one 802.1x-EAP regardless of how many L3 handovers occur. Therefore, the proposed scheme reduces the handover latency that results from a lengthy 802.1x-based EAP. The proposed key management and security scheme is extensively analyzed in terms of security and performance, and the proposed security scheme is shown to be more secure than those that were previously proposed.

1. Introduction

Mobile IPv6 Fast Handover (FMIPv6) [1] has been proposed in order to minimize the delay induced by handover operations of *Mobile IPv6* [2]. When a wireless Mobile Node (MN) changes its attachment point to a new Access Router (AR), it is possible to provide IP connectivity in advance of the actual registration of the mobile IP by tunneling data between the current and the target access routers. The basic idea behind FMIPv6, which is a kind of Layer Three (L3) handover, is to leverage information from Layer Two (L2) technologies, such as IEEE 802.11 [3], to either predict or rapidly respond to a handover event. On the other hand, a wireless MN attached to an AR via an Access Point (AP) can move to a new AP without changing its attachment to the AR. In this case an L2 handover occurs, and the MN must reassociate and authenticate with the new AP using IEEE 802.1x-based Extensible Authentication Protocol (802.1x-EAP) [4]. Given that an L2 handover is also induced when an L3 handover occurs, IEEE 802.11-based FMIPv6 [5] has been proposed and has been analyzed in terms of its handover latency [6, 7].

There are two security issues associated with IEEE 802.11-based FMIPv6. One issue is that of establishing an L3 key between an MN and a new AR on each L3 handover. Based on the L3 key, the L3 signaling messages used to establish the tunnel between the current AR and the target AR can be authenticated. in particular, a compromise of the current L3 key should not induce that of the future L3 key to suppress the domino effect. Several security mechanisms [8–10] have been previously proposed to establish the L3 key. However, they have several weaknesses in terms of security and efficiency. The other issue is to reduce the authentication delay caused by the L3 handover. The MN would perform a lengthy 802.1x-EAP authentication with AAA (Authentication, Authorization, and Auditing) server on each L3 handover inducing the L2 handover. As a result of successful 802.1x-EAP authentication, the L2 key is shared and used for mutual authentication between the MN and a new AP. Since both L2 and L3 keys are generated and managed independently, key management for IEEE 802.11-based FMIPv6 becomes complex. A simplified key management scheme [10] to derive the L2 key from the L3 key has been proposed to reduce the authentication delay.

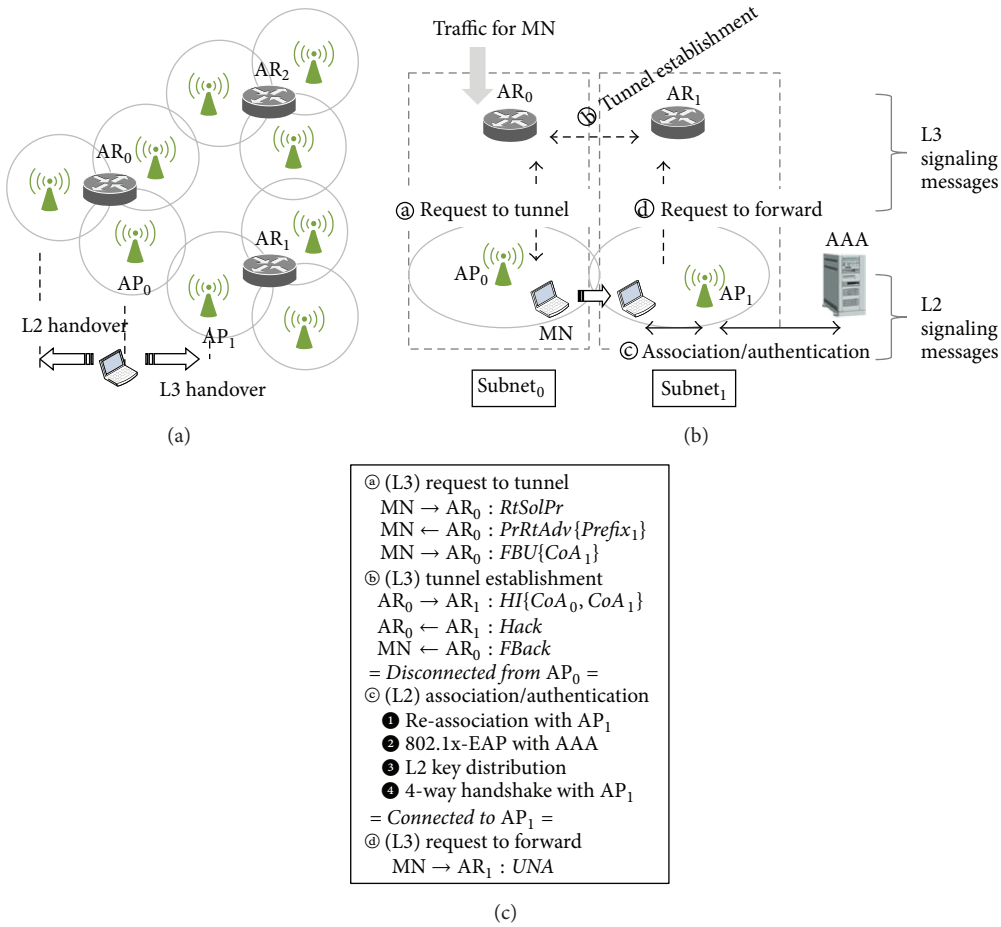


Figure 1: L3 handover procedure of IEEE 802.11-based FMIPv6.

However, it is still required for the MN to be interconnected with the AAA on each L3 handover, and it has a security problem in that a session hijacking attack is feasible, which will be shown in this paper.

A new key management and security scheme is proposed to secure IEEE 802.11-based FMIPv6 signaling messages. A contribution of this paper is twofold: first, a new L3 key establishment scheme is proposed, which is secure against a variety of session hijacking and redirection attacks in case of an L3 key compromise. Second, unlike the original IEEE 802.11-based FMIPv6 where the MN would perform a full IEEE 802.1x-EAP authentication with the AAA on each L3 handover, the newly proposed scheme requires only one IEEE 802.1x-EAP authentication regardless of how many L3 handovers occur. Therefore, the proposed scheme reduces the handover latency that results from the lengthy IEEE 802.1x-EAP authentication. In particular, the proposed key management scheme is of a cross-layer type in the sense that the L2 keys are derived from the L3 key. In Section 2, the background of FMIPv6 over IEEE 802.11 WLAN is introduced along with related works. A new key management and security scheme is proposed in Section 3. The new scheme is analyzed and compared with previous schemes in terms of security and performance in Sections 4 and 5. Finally, concluding remarks are given in Section 6.

2. FMIPv6 over IEEE 802.11 WLAN and Related Works

2.1. FMIPv6 over IEEE 802.11 WLAN. We consider a network environment of Figure 1(a), where each subnet of the AR is comprised of one or more APs. When the MN moves from AP_0 to AP_1, then both L3 and L2 handovers occur. Namely, the MN's subnet changes from $subnet_0$ to $subnet_1$.

Suppose an L2 handover from AP_0 to AP_1 is anticipated as in Figure 1(b). By exchanging both the Router Solicitation for Proxy Advertisement (*RtSolPr*) and the Proxy Router Advertisement (*PrRtAdv*) messages, the MN configures a new care-of-address (CoA), CoA_1, according to the subnet prefix, $Prefix_1$, of AR_1. Then, the MN sends a Fast Binding Update (*FBU*) message to request AR_0 to forward packets destined for the MN to AR_1, (ⓐ in Figure 1(c)). A tunnel is established between AR_0 and AR_1 by exchanging Handover Initiate (*HI*) and Handover Acknowledgment (*Hack*) messages (ⓑ in Figure 1(c)), where the *HI* message carries the current CoA of the MN, CoA_0, and a new CoA, CoA_1, to be used on

a subnet of AR_1. The packets for the MN start to flow to and are buffered at AR_1. Then, a Fast Binding Acknowledgment (*FBack*) message is sent to the MN to notify of the completion of the tunnel establishment.

When finally disconnected from AP_0, namely, when the L2 handover occurs, the MN reassociates with AP_1 (❶ in Figure 1(c)) and performs a full IEEE 802.1x-EAP authentication with the AAA (❷ in Figure 1(c)). If it is successful, L2 key distribution starts based on the MSK_1 shared between the MN and AAA. The PMK_1 truncated from the MSK_1 is securely distributed to AP_1 (❸ in Figure 1(c)). Subsequently, a 4-*way Handshake* (❹ in Figure 1(c)) based on PMK_1 is performed between the MN and AP_1. At this point, the MN is successfully attached to a subnet of AR_1 ($subnet_1$) through AP_1. Finally, the MN sends an Unsolicited Neighbor Advertisement (*UNA*) message to request AR_1 to deliver the buffered packets forwarded from AR_0 (ⓓ in Figure 1(c)). The fields inherent to the L3 signaling messages (e.g., *RtSolPr*) are intentionally omitted for the sake of providing a simple explanation. Instead, they will be padded with the security-related fields when discussing the mechanism used to secure them.

2.2. Threat Models and Problem Statements. Without proper protection for L3 signaling messages in FMIPv6 (ⓐ and ⓓ in Figure 1), an adversary can forge or modify them to mount a variety of redirection attacks. Unless the previous AR (AR_0 in Figure 1) can verify that the *FBU* message comes from an authorized MN, legitimate traffic for the MN might be redirected to the adversary. Furthermore, the packets for the MN can be redirected to any other host to execute a flooding attack against it or against the subnet to which it belongs. The adversary can also forge the *UNA* message to steal the traffic destined for the legitimate MN. In order to avoid the above attacks, security associations should be established between the MN and ARs. An L3 key shared between the MN and AR_0 is used to authenticate the L3 signaling messages of ⓐ in Figure 1, while the L3 signaling messages of ⓓ in Figure 1 can be authenticated based on another L3 key shared between the MN and AR_1. Therefore, it is necessary to embed L3 key distribution protocol into the original 802.11-based FMIPv6. In particular, the domino effect should be suppressed in case of the L3 key compromise. Namely, the compromise of the current L3 key should not induce that of the future L3 key. On the other hand, the 802.1x-EAP authentication (❷ in Figure 1) is for the MN to share a new L2 key with the new AP attached to the target AR through AAA. The L2 key is used for mutual authentication between the MN and the new AP. However, the authentication delay caused by the 802.1x-EAP is a major source of the handover delay, since 8 messages should be exchanged between the MN and AAA in case of using EAP-Transport Layer Security (TLS) method. Hence, if the 802.1x-EAP can be skipped on each L3 handover of the IEEE 802.11-based FMIPv6, the overall handover delay can be greatly improved.

2.3. Previous Works. Several security schemes [11–13] have been investigated for sharing the L2 key to protect L2 signaling messages, which are based on a concept of ticket, key hiding technique, and authentication server, respectively. On the other hand, a security scheme [8] based on Cryptographically Generated Address (CGA) has been proposed to secure L3 signaling messages (ⓐ in Figure 1). CGA is formed by taking the IPv6 subnet prefix for a node's subnet and combining it with an interface identifier suffix formed as the hash of the node's public key. The L3 key, K_0, generated by AR_0 is encrypted using the public encryption key of MN, ePK_{MN}, and it is sent to the MN. Both *RtSolPr* and *PrRtAdv* messages are protected by the digital signature while the *FBU* message is protected by the symmetric key. The definition of the notations is shown in Notations section. Consider

$$\begin{aligned}
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{: } RtSolPr\,\{PK_{\mathrm{MN}}, ePK_{\mathrm{MN}}, Nonce,\\
&\quad Sig\,(SK_{\mathrm{MN}})\}\\
&\mathrm{MN} \longleftarrow \mathrm{AR}_0\text{: } PrRtAdv\,\{Prefix_1, [K_0]\,ePK_{\mathrm{MN}}, Nonce,\\
&\quad Sig\,(SK_{\mathrm{AR}_0})\}\\
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{: } FBU\,\{CoA_1, MAC\,(K_0)\}\,.
\end{aligned} \tag{1}$$

However, the security scheme does not provide a method to establish a security association between the MN and the target router AR_1, so that the *UNA* message cannot be protected and can be forged to steal the traffic destined for the legitimate MN. Furthermore, a variety of DoS (Denial of Service) attacks can be mounted using the unauthenticated *UNA* message, which has also been mentioned in [14]. Another security scheme [9] has been proposed to protect L3 signaling messages including the *UNA* message. The security schemes proposed in [8, 9] are only for protecting L3 signaling messages (ⓐ and ⓓ in Figure 1).

Integrated handover authentication scheme [10] has been proposed to integrate the L3 key with the L2 key; namely, the L2 key can be derived directly from the L3 key. Before the MN handovers to the target AR, the MN transports a new L3 key, K_1, to AR_1 through the AAA as in (2), where *MSK* is a secret key shared between the MN and AAA. Subsequently, AR_1 distributes the L2 key (PMK_1) derived from the L3 key (K_1) to the new AP. A current L3 key, K_0, is used to secure the L3 signaling messages (ⓐ in Figure 1), while a new L3 key, K_1, is for securing the L3 signaling messages (ⓓ in Figure 1). Consider

$$\begin{aligned}
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{:}\\
&\quad \{[K_1]_{MSK}, R_{\mathrm{MN}}, MAC\,(MSK), MAC\,(K_0)\}\\
&\mathrm{AR}_0 \longrightarrow \mathrm{AR}_1\text{: } \{[K_1]_{MSK}, R_{\mathrm{MN}}, MAC\,(MSK)\}\\
&\mathrm{AR}_1 \longrightarrow \mathrm{AAA}\text{: } \{[K_1]_{MSK}, R_{\mathrm{MN}}, MAC\,(MSK)\}\\
&\mathrm{AR}_1 \longleftarrow \mathrm{AAA}\text{: } \{[K_1]_{MSK}, R_{\mathrm{MN}}\}\,.
\end{aligned} \tag{2}$$

As mentioned in Section 2.2, it is desirable for the interaction with the AAA to be skipped in order to speed up the handover process. However, it has not actually been skipped; instead, it has been placed on the L3 protocol. Furthermore, it is not secure against the L3 key compromise attack. Namely, the

domino effect occurs in that if K_0 is compromised, then K_1 is also compromised. The security weakness will be more discussed in Section 4.4.

3. The Proposed Key Management and Security Scheme

A new cross-layer scheme for key management and associated security is proposed, where an L2 key is derived from an L3 key to speed up the L3 handover procedure accompanying the L2 handover, so that it is similar to the one in [10]. However, there is much difference between them in terms of security and efficiency. It is assumed that preestablished security associations exist between AR_0 and AR_1, AR and AP. A security association between the MN and AAA is also assumed to exist for the initial access of MN to the network. The notations used in this paper are shown in Notations section.

3.1. Design Principles. Suppose an MN handover from a subnet of AR_0 to that of AR_1. Two L3 keys are required to protect the L3 signaling messages: the one (K_0) on the subnet of AR_0 and the other (K_1) on the subnet of AR_1. Unlike the previous schemes [8–10] based on the interaction with AAA, the MN generates and distributes K_1 proactively to AR_1 before it moves from AR_0 to AR_1. Furthermore, the L2 key (PMK_1) can be derived from K_1 on the subnet of AR_1 and pushed into new AP_1 attached to AR_1, so that the IEEE 802.1x-EAP can be skipped.

Since a new L3 key (K_1) to be used after handover is predistributed to AR_1 by the MN, it is important to guarantee that a compromise of the current L3 key (K_0) does not induce that of the future L3 key (K_1); namely, the domino effect should be suppressed. For this purpose, double public-key encryptions are applied to K_1 before distribution: the one with the public key of AR_1 and the other with that of AR_0. In our proposed protocol, the authenticity of the public key of AR_1 is protected by K_0. However, if K_0 is compromised, K_1 can also be exposed to an adversary. Therefore, it is also protected by the public key of AR_0 which has been provided to the MN during the previous handover session.

An IPv6 address of the MN on the subnet of AR_i is formed as CoA_i ($= Prefix_i \parallel IID_i$), where IID_i is an 64-bit interface identifier. There are two ways of configuring IID: the typical one is based on the L2 address of the MN, and the other is using a random number as IID. In our proposed protocol, we also use the random number, but in a slightly different way. It is derived as follows: $IID_i = h_{64}(r_i)$ based on a random number r_i selected by the MN. When moving from AR_i to AR_{i+1}, the MN should reveal the random number r_i to prove that CoA_i was generated and owned by the MN. So CoA_i plays a role of a commitment. A main reason to use this mechanism is to defend against a session hijacking attack when the current L3 key is compromised.

3.2. Initial Network Access Protocol. When the MN *initially* associates with AP_0 to access the network service (❶ in Figure 2), it performs full IEEE 802.1x-EAP authentication with the AAA (❷ in Figure 2). As a result, the MSK_0 is shared between them, and the information (AR_0 and ePK_{AR_0}) for the default router of the MN is passed to the MN. Subsequently, the AAA derives two L3 keys IK and K_0 which are truncated from MSK_0 and transports them with MN_{NAI} securely to the default router, where MN_{NAI} is the Network Access Identifier (NAI) of the MN. IK is an initial L3 configuration key, while K_0 is an L3 handover key, based on which an L2 key (PMK_0) is also derived. Then, AR_0 pushes $PMK_0 = kdf(K_0, MN, AP_0)$ into AP_0 (❸ in Figure 2).

MN and AP_0 denote the L2 addresses of the MN and AP_0, while AR_0 denotes the L3 addresses of AR_0. The 4-*way Handshake* based on the PMK_0 is executed between the MN and AP_0 in order for the MN to attach to a subnet of AR_0 (subnet_0) through AP_0 (❹ in Figure 2). Finally, the MN performs an L3 configuration to check whether its IPv6 care-of-address, CoA_0, is duplicate on the subnet of AR_0:

$$\begin{aligned}
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\colon RtSol\,\{R_{\mathrm{MN}}, MN_{\mathrm{NAI}}, MAC\,(IK)\}\\
&\mathrm{MN} \longleftarrow \mathrm{AR}_0\colon RtAdv\,\{R_{\mathrm{MN}}, R_0, Prefix_0, MAC\,(IK)\}\\
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\colon Conf\,\{R_0, CoA_0, MAC\,(IK)\}\,.
\end{aligned} \tag{3}$$

The MN sends an *Router Solicitation* (*RtSol*) message to AR_0. Based on MN_{NAI}, AR_0 can retrieve IK and can respond to the *RtSol* message by sending a *Router Advertisement* (*RtAdv*) message. The *RtAdv* message contains the subnet prefix of AR_0, $Prefix_0$, from which the MN configures CoA_0 ($= Prefix_0 \parallel IID_0$), and the MN then sends a *Configuration* (*Conf*) message where the interface identifier $IID_0 = h_{64}(r_0)$ is computed based on a random number r_0 generated by the MN. If CoA_0 is verified to be unique on the subnet, the initial network access protocol is successfully terminated. Eventually, (CoA_0, K_0) is stored into the neighbor cache of AR_0.

3.3. Proposed Secure Handover Procedure. Suppose an L2 handover accompanying an L3 handover occurs from AP_0 to AP_1. A sequence of signaling messages is shown in Figure 3, where the L3 key, K_0, at the subnet_0 has already been shared between the MN and AR_0 as a result of a previous handover process or an initial network access. After receiving the *RtSolPr* message, AR_0 responds by sending a *PrRtAdv* message with a subnet prefix of AR_1 ($Prefix_1$) and the public key of AR_1 (ePK_{AR_1}):

$$\mathrm{MN} \longrightarrow \mathrm{AR}_0\colon RtSolPr\,\{R_{\mathrm{MN}}, MAC\,(K_0)\} \tag{4}$$

$$\begin{aligned}
&\mathrm{MN} \longleftarrow \mathrm{AR}_0\colon PrRtAdv\,\big\{R_{\mathrm{MN}}, R_0, Prefix_1, ePK_{\mathrm{AR}_1},\\
&\quad MAC\,(K_0)\big\}
\end{aligned} \tag{5}$$

$$\begin{aligned}
&\mathrm{MN} \longrightarrow \mathrm{AR}_0\colon FBU\,\big\{R_0, CoA_1,\\
&\quad \big[r_0, [CoA_1, K_1]\,ePK_{\mathrm{AR}_1}\big]\,ePK_{\mathrm{AR}_0}, MAC\,(K_0)\big\}\,.
\end{aligned} \tag{6}$$

After configuring CoA_1 ($= Prefix_1 \parallel IID_1$), where $IID_1 = h_{64}(r_1)$ is computed based on a random number r_1, the MN generates a new L3 key, K_1, and sends an *FBU* message

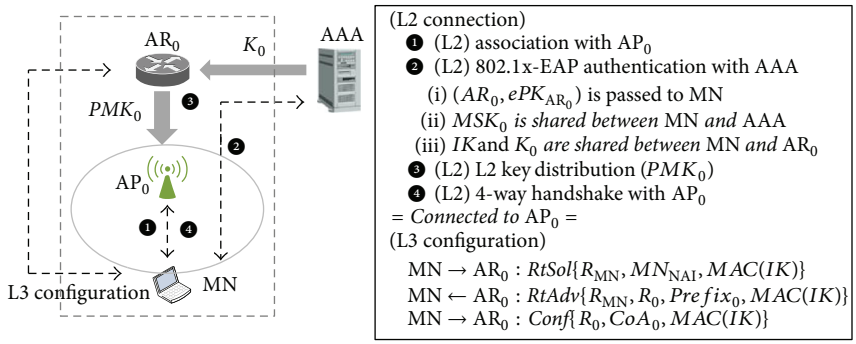


FIGURE 2: Proposed initial network access protocol.

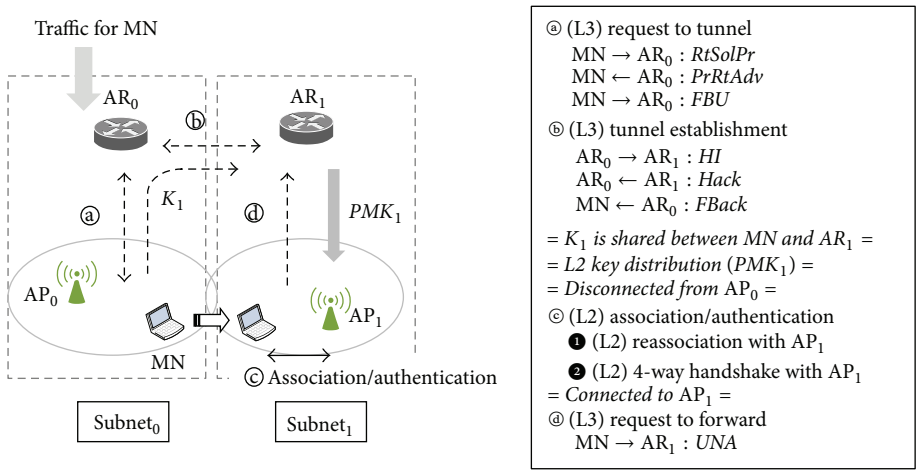


FIGURE 3: Proposed secure handover protocol.

to AR_0 (ⓐ in Figure 3). Since K_1 is to be shared with AR_1, it is first encrypted with the public key of AR_1, ePK_{AR_1}, subsequently encrypted with the public key of AR_0, ePK_{AR_0}. When receiving the *FBU* message, AR_0 first obtains $\{r_0, [CoA_1, K_1]ePK_{AR_1}\}$ after decryption, in order to check if $h_{64}(r_0)$ is equal to IID_0 of CoA_0. If not, the message is proven to be not sent from the MN whose IPv6 address is CoA_0 and the handover protocol is aborted. Otherwise, the L3 key, K_0, is eventually passed to the target AR_1 for the purpose of sharing it with the MN at the subnet$_1$. A reason to encrypt K_1 twice is to defend against an L3 key compromise attack, which will be more discussed in Section 4.3. Consider

$$\begin{aligned} &\text{A secure channel between } AR_0 \text{ and } AR_1 \\ &HI\left\{CoA_0, CoA_1, [CoA_1, K_1]\, ePK_{AR_1}\right\} \\ &Hack\,\{\} \\ &MN \longleftarrow AR_0\text{: } FBack\,\{MAC\,(K_0)\} \\ &MN \longrightarrow AR_1\text{: } UNA\,\{MAC\,(K_1)\}\,. \end{aligned} \tag{7}$$

The target router AR_1 obtains K_1 through the *HI* message after decryption, and K_1 will be used to derive the L2 key $PMK_1 = kdf(K_1, MN, AP_1)$ and to secure the future L3 handover. AR_1 pushes PMK_1 into AP_1.

After reassociating with AP_1 (❶ in Figure 3), the MN performs a 4-*way Handshake* (❷ in Figure 3) based on PMK_1 without IEEE 802.1x-EAP authentication with the AAA. Subsequently, the MN sends an *UNA* message to request AR_1 to deliver the buffered packets forwarded from AR_0 (ⓓ in Figure 3). (CoA_1, K_1) is finally stored into the neighbor cache of AR_1.

4. Security Analysis and Comparisons

4.1. Comparison of Key Management Schemes. In this Section, three key management schemes are compared: security-enhanced IEEE 802.11-based FMIPv6 [8, 9], Integrated Scheme [10], and our proposed scheme, which are denoted as Schemes 1, 2, and 3, respectively. In case of Scheme 1, the security mechanisms [8, 9] to secure the L3 signaling messages are added to the original IEEE 802.11-based FMIPv6 [5]. However, there are no key management in that both L3 and L2 keys are separately generated and maintained, meaning that IEEE 802.1x-EAP authentication (ⓒ in Figure 4(a)) should be performed on each L3 handover. A method to integrate the L3 key with the L2 key has been proposed in Scheme 2. Before the MN moves to a new AP attached to the target subnet AR_1, it requests the AAA to transport a new L3 key (K_1) to AR_1, and then a new L2 key (PMK_1)

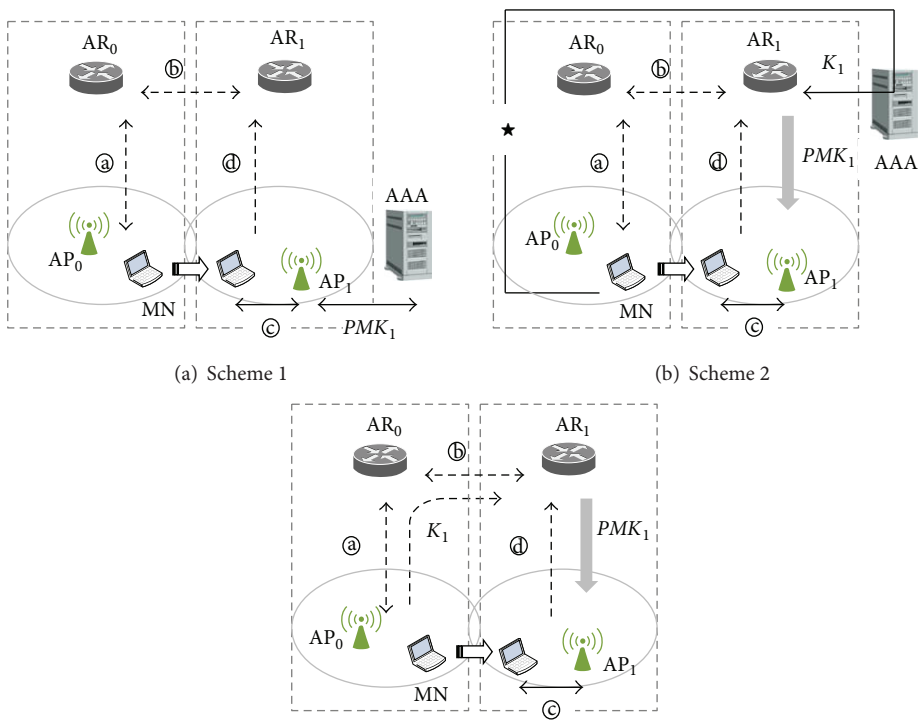


Figure 4: Comparison of key management schemes.

derived from it is pushed into AP_1 (★ in Figure 4(b)). But the interaction with the AAA cannot be skipped either during the L3 handover. On the other hand, in the proposed scheme (Scheme 3) of Figure 4(c), IEEE 802.1x-EAP authentication is performed only once during the initial network access in Figure 1. During a handover from AR_0 to AR_1, a new L3 key is sent to AR_1 via AR_0. Therefore, both the MN and AR_1 share K_1, which can be used to secure L3 signaling messages and to derive a new L2 key (PMK_1) in the target subnet. Since K_1 is proactively distributed to AR_1 before the MN moves from AR_0 to AR_1, the MN can perform a 4-*way Handshake* immediately after reassociating with AP_1 (ⓒ in Figure 4(c)).

4.2. Replay and Redirection Attacks. In order to guarantee the freshness of FMIPv6 signaling messages, to be precise, to protect from a replay attack, challenge-response authentication based on the random numbers (R_{MN} and R_0) is employed for our proposed scheme. A scenario to which the replay attack is applied is as follows: the MN is attached again to AR_0 at handover session i, while it has been attached to the same AR_0 at handover session j, ($i > j$). Suppose the MN has moved to AR_1 during the handover session j and plans now to move to AR_2 during the handover session i. In this case, an adversary can try to replay the FMIPv6 signaling messages used during the handover session j to redirect the traffic for the MN. However, the replay attack is not successful due to both nonce values and the L3 key which is unique for each handover session.

4.3. Compromised L3 Key and Session Hijacking Attack. A case of the L3 key compromise is considered in this section. We show that our proposed scheme is secure against a session hijacking attack through redirection even though the current L3 key, K_0, of (5) and (6) is exposed to an adversary. To protect the *FBU* message in Section 3.3, our proposed security scheme employs two public-key encryptions with ePK_{AR_0} and ePK_{AR_1} as in (5) and (6).

The MN obtains the public key of AR_0 (ePK_{AR_0}) as a result of an initial network access or a previous L3 handover, while the public key of AR_1 (ePK_{AR_1}) is passed to the MN by AR_0.

4.3.1. Session Hijacking by Redirection Attack. Suppose an adversary $A_{(MN)}$ disguising a victim MN knows the current L3 key K_0 and starts an L3 handover as follows:

$$A_{(MN)} \longrightarrow AR_0\colon RtSolPr\left\{R^*_{MN}, MAC\left(K_0\right)\right\} \tag{11$'$}$$

$$A_{(MN)} \longleftarrow AR_0\colon PrRtAdv\left\{R^*_{MN}, R_0, Prefix_1, ePK_{AR_1}, MAC\left(K_0\right)\right\} \tag{12$'$}$$

$$A_{(MN)} \longrightarrow AR_0\colon FBU\left\{R_0, CoA^*_1, \left[r^*_0, \left[CoA^*_1, K_1\right] ePK_{AR_1}\right] ePK_{AR_0}, MAC\left(K_0\right)\right\}. \tag{13$'$}$$

R^*_{MN}, CoA^*_1, and r^*_0 are generated by $A_{(MN)}$ that tries to hijack the current traffic for the MN (CoA_0) and forward it to $A_{(MN)}$ (CoA^*_1). When receiving the *FBU* message, AR_0

obtains r_0^* after decryption and verifies if IID_0 of the source IPv6 address (CoA_0) is identical to $h_{64}(r_0^*)$. If the verification is not successful, the protocol stops. Since $h_{64}(\cdot)$ is based on a one-way hash function and the r_0 used to derive IID_0 is known only to the MN, all the adversary can do is attempt to guess r_0 (the probability of $r_0 = r_0^*$ is 2^{-64}). Since CoA_0 is valid only on the subnet$_0$ and keeps changing as the MN moves, the probability is negligible enough to defend against such an attack.

4.3.2. Session Hijacking by Man-in-the-Middle Attack. Suppose an adversary $\mathrm{A}_{(\mathrm{MN})}$ knows the current L3 key K_0 and the victim MN starts an L3 handover to request AR_0 to forward its traffic to CoA_1. To see why the public-key encryption with ePK_{AR_0} is required, (6) is modified into (13″):

$$\begin{aligned}\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{: } FBU \{&R_0, CoA_1, r_0,\\ &[CoA_1, K_1]\, ePK_{\mathrm{AR}_1}, MAC(K_0)\}.\end{aligned} \tag{13″}$$

Then, the adversary can mount a man-in-the-middle attack as follows:

$$\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{: } RtSolPr\{R_{\mathrm{MN}}, MAC(K_0)\} \tag{8}$$

$$\begin{aligned}\mathrm{A}_{(\mathrm{MN})} \longleftarrow \mathrm{AR}_0\text{: } PrRtAdv \{&R_{\mathrm{MN}}, R_0, Prefix_1, ePK_{\mathrm{AR}_1},\\ &MAC(K_0)\}\end{aligned} \tag{9}$$

$$\begin{aligned}\mathrm{MN} \longleftarrow \mathrm{A}_{(\mathrm{MN})}\text{: } PrRtAdv \{&R_{\mathrm{MN}}, R_0, Prefix_1, ePK^*_{\mathrm{AR}_1},\\ &MAC(K_0)\}\end{aligned} \tag{10}$$

$$\begin{aligned}\mathrm{MN} \longrightarrow \mathrm{A}_{(\mathrm{MN})}\text{: } FBU \{&R_0, CoA_1, r_0,\\ &[CoA_1, K_1]\, ePK^*_{\mathrm{AR}_1}, MAC(K_0)\}\end{aligned} \tag{11}$$

$$\begin{aligned}\mathrm{A}_{(\mathrm{MN})} \longrightarrow \mathrm{AR}_0\text{: } FBU \{&R_0, CoA_1^*, r_0,\\ &[CoA_1^*, K_1]\, ePK_{\mathrm{AR}_1}, MAC(K_0)\}.\end{aligned} \tag{12}$$

Namely, $\mathrm{A}_{(\mathrm{MN})}$ observing between the MN and AR_0 modifies ePK_{AR_1} of (9) into $ePK^*_{\mathrm{AR}_1}$ of (10) generated by $\mathrm{A}_{(\mathrm{MN})}$, so that $\mathrm{A}_{(\mathrm{MN})}$ can obtain a new L3 key K_1 and hijack the traffic for CoA_1 for the purpose of forwarding it to CoA_1^*. Eventually, the connection with AR_1 is turned over to $\mathrm{A}_{(\mathrm{MN})}$. On the other hand, if (6) is used instead of (13′), (11) and (12) are changed into (19′) and (20′), respectively:

$$\begin{aligned}\mathrm{MN} \longrightarrow \mathrm{A}_{(\mathrm{MN})}\text{: } FBU \{&R_0, CoA_1,\\ &[r_0, [CoA_1, K_1]\, ePK^*_{\mathrm{AR}_1}]\, ePK_{\mathrm{AR}_0}, MAC(K_0)\}\end{aligned} \tag{19′}$$

$$\begin{aligned}\mathrm{A}_{(\mathrm{MN})} \longrightarrow \mathrm{AR}_0\text{: } FBU \{&R_0, CoA_1,\\ &[r_0, [CoA_1, K_1]\, ePK^*_{\mathrm{AR}_1}]\, ePK_{\mathrm{AR}_0}, MAC(K_0)\}.\end{aligned} \tag{20′}$$

When intercepting (19′), $\mathrm{A}_{(\mathrm{MN})}$ cannot modify CoA_1 or obtain K_1 since they are encrypted with ePK_{AR_0}. Therefore, when receiving $[CoA_1, K_1]ePK^*_{\mathrm{AR}_1}$ through the *HI* message, AR_1 aborts the current protocol since it cannot be decrypted with ePK_{AR_1}. Therefore, a compromise of the current L3 key does not induce that of the future L3 key.

4.4. Security Comparisons. Table 1 shows security comparisons (Schemes 1, 2, and 3) including the key management comparisons discussed in Section 4.1. It has been shown that our proposed scheme is secure against the session hijacking attack in case of the L3 key compromise. Scheme 1 is also secure since the L3 key is always generated and shared as a result of 802.1x-EAP protocol. However, Scheme 2 ((2) in Section 2.3) is not secure when the L3 key is compromised. Suppose K_0 is exposed to an adversary $\mathrm{A}_{(\mathrm{MN})}$ and (13) can be observed from the previous handover session:

$$\begin{aligned}&\text{previous handover session with L3 key } K_X\\ &\mathrm{MN} \longrightarrow \mathrm{AR}_0\text{: } \{[K_0]_{MSK}, R_{\mathrm{MN}}, MAC(MSK), MAC(K_X)\}\\ &\qquad\vdots\end{aligned} \tag{13}$$

$$\begin{aligned}&\text{current handover session with L3 key } K_0 \text{ (compromised)}\\ &\mathrm{A}_{(\mathrm{MN})}\\ &\quad\longrightarrow \mathrm{AR}_0\text{: } \{[K_0]_{MSK}, R_{\mathrm{MN}}, MAC(MSK), MAC(K_0)\}.\end{aligned} \tag{14}$$

In this case, if the adversary replays a part of (13) as in (14) with the compromised L3 key K_0, then the adversary can share the same L3 key with a new AR, so that the adversary can hijack the current session.

4.5. AAA Issues for Security and Billing. FMIPv6 can support handover across different administrative domains. As mentioned before, if the two ARs belong to two different administrative domains, there should be a prior roaming agreement between them for security and billing. Typically, the accounting data (information about MN's resource consumption) collected by the network devices in the visiting domain is carried by the accounting protocol to the home domain. FMIPv6 over IEEE 802.11 is followed by the MIPv6 BU (Binding Update) protocol whose role is to inform MN's HA (Home Agent) of the current AR. There are two service providers, Network Access Service Provider (NSP) and Mobility Service Provider (MSP), in MIPv6 bootstrapping environment [15]. The IEEE 802.11-based FMIPv6 service can be provided by the NSP offering a basic network access service to MN, while the MIPv6 BU service is provided by the MSP. So when the MIPv6 BU protocol is initiated, MSP's authorizer (AAA) will be interacted with the MN and AR, which is beyond the scope of this paper.

5. Performance Analysis and Comparison

In this section, the three handover latencies from the previous schemes (Schemes 1 and 2) and from the proposed scheme (Scheme 3) are compared. We first describe the analytical mobility model for the performance evaluation, and then we

Table 1: Security comparisons.

	Scheme 1		Scheme 2	Scheme 3
	[8]	[9]	[10]	[proposed one]
L3/L2 key management	None	None	Yes	Yes
Interaction with AAA	Required	Required	Required	Not required
L3 key generation	by AR	by MN	by MN	by MN
L2 key generation	802.1x-EAP	802.1x-EAP	from L3 key	from L3 key
Protection for UNA	None	Provided	Provided	Provided
Security attack due to L3 key compromise	Secure	Secure	Insecure	Secure

analyze and compare the handover costs and the numeric results of the analysis.

5.1. Analytical Mobility Model. For the sake of simplicity, a square-shaped network model is used to analyze and compare the performance of the protocol under the three different schemes. In the square-shaped network model, coverage of the entire administrative domain and that of each AP are all square-shaped, and N APs are uniformly distributed over the area of the administrative FMIPv6 domain. Figure 5 shows the square-shaped mobility model where the bold lines indicate the boundary of the subnet consisting of 4 APs (AP_{01}, AP_{02}, AP_{03}, and AP_{04}) connected to AR_0.

The handover procedure is performed by the MN between ARs and APs. Hence, the handover rate is closely related to the mobility pattern of MN. The Fluid Flow (FF) model is widely used to analyze issues related to cell boundary crossing, such as a handover [16]. The FF model is suitable for MNs with a static speed and direction of motion. We adapt the FF model for use as the mobility model. Let l and L denote the perimeter of each AP and AR, while v and p, respectively, denote the average velocity and density of MN. The MNs are uniformly distributed with a density p, and they move at an average velocity of v in directions that are uniformly distributed over $[0, 2\pi]$. In the next analysis, v is varied from 0.1 m/s to 5 m/s and p is set to 0.0002 MNs/m^2 (200 MNs per Km^2). Let R_c and R_d be the crossing rates over the coverage of each AP and AR, respectively. They are then defined as follows:

$$R_c = \frac{pvl}{\pi}, \qquad R_d = \frac{pvL}{\pi}, \quad \left(\text{where } L = l\sqrt{N}\right). \tag{15}$$

5.2. Handover Cost Analysis and Numerical Results. In IEEE 802.11-based FMIPv6, an MN performs L2 and L3 handover procedures. When an MN changes its current address to a new AR, the MN performs an L3 handover procedure. On the other hand, if an MN changes its current AP to another one connected to the same AR, then MN performs an L2 handover procedure. In this section, the average handover cost per MN is defined as the sum of the cost of the L3 handover and the cost of the L2 handover per unit time in order to provide results for the performance comparison. Let A_j be the average handover cost per MN in unit of time, and I_j and H_j are the L3 handover cost and the L2 handover cost for Scheme j (= 1, 2, 3), respectively. I_j and H_j are defined as the sum of the signaling cost S_j and the processing cost P_j for the L3 and L2 handovers, respectively. Based on (15), the average handover cost per MN, A_j, can be calculated as follows [16], where W_{AR} is the area of an AR domain:

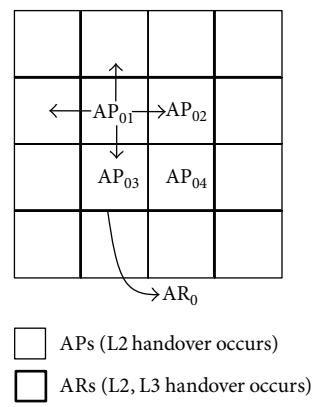


Figure 5: Square-shaped mobility model ($N = 4$).

$$A_j = \frac{\left(R_d \cdot I_j + \left(N \cdot R_c - R_d\right) \cdot H_j\right)}{\left(p \cdot W_{AR}\right)}, \quad \left(\text{where } I_j\left(H_j\right) = S_j + P_j\right). \tag{16}$$

The parameter descriptions and values for the performance comparison, referenced from [16], are defined in Table 2. Note that the values other than p, v, l, and N are defined "relatively" for the purpose of this comparison, so the handover cost does not indicate the actual authentication delay for the corresponding scheme.

Using the parameters in Table 2, the L2 and L3 handover costs and the average handover cost can be calculated based on (17). The P_{jMN}, P_{jAP}, P_{jAR_0}, P_{jAR_1}, and P_{jAAA} indicate the processing costs on MN, AP, AR_0, AR_1, and AAA, respectively, of Scheme j, and each of them is also calculated from the cost of cryptographic operations such as C_{key} and C_{hash}. Let the number of hops between any two relatively close

Table 2: Parameters for evaluation.

Symbol	Description	Value
p	Density in a cell (MNs/m^2)	0.0002 MNs/m^2
v	Average velocity of an MN (m/s)	5 m/s (0.1~5)
l	Perimeter of AP's coverage (m)	120 m
N	Number of APs in an AR	5 APs (1~10)
C_{enc} C_{dec}	Encryption cost/decryption cost	1
C_{key}	Key generation cost	1
C_{int}	Message integrity code cost	0.25
C_{hash}	Hash cost	0.25
C_{kdf}	KDF cost	0.25
C_{rand}	Random number generation cost	0.25
C_{hop}	Transmission cost on the hop	10
C_{pub}	Public key operation cost	10
C_{wired}	Unit of transmission cost for a wired link	1
C_{wireless}	Unit of transmission cost for a wireless link	1.5
$D_{\text{AP-AAA}}$	Number of hops between AP and AAA	10
$D_{\text{AP-AR}}$	Number of hops between AP and AR	2

network devices (such as MN-to-AP, AP-to-AP, and AR-to-AR) be 1. a_{ji} and b_{jk} are specific coefficients of Scheme j:

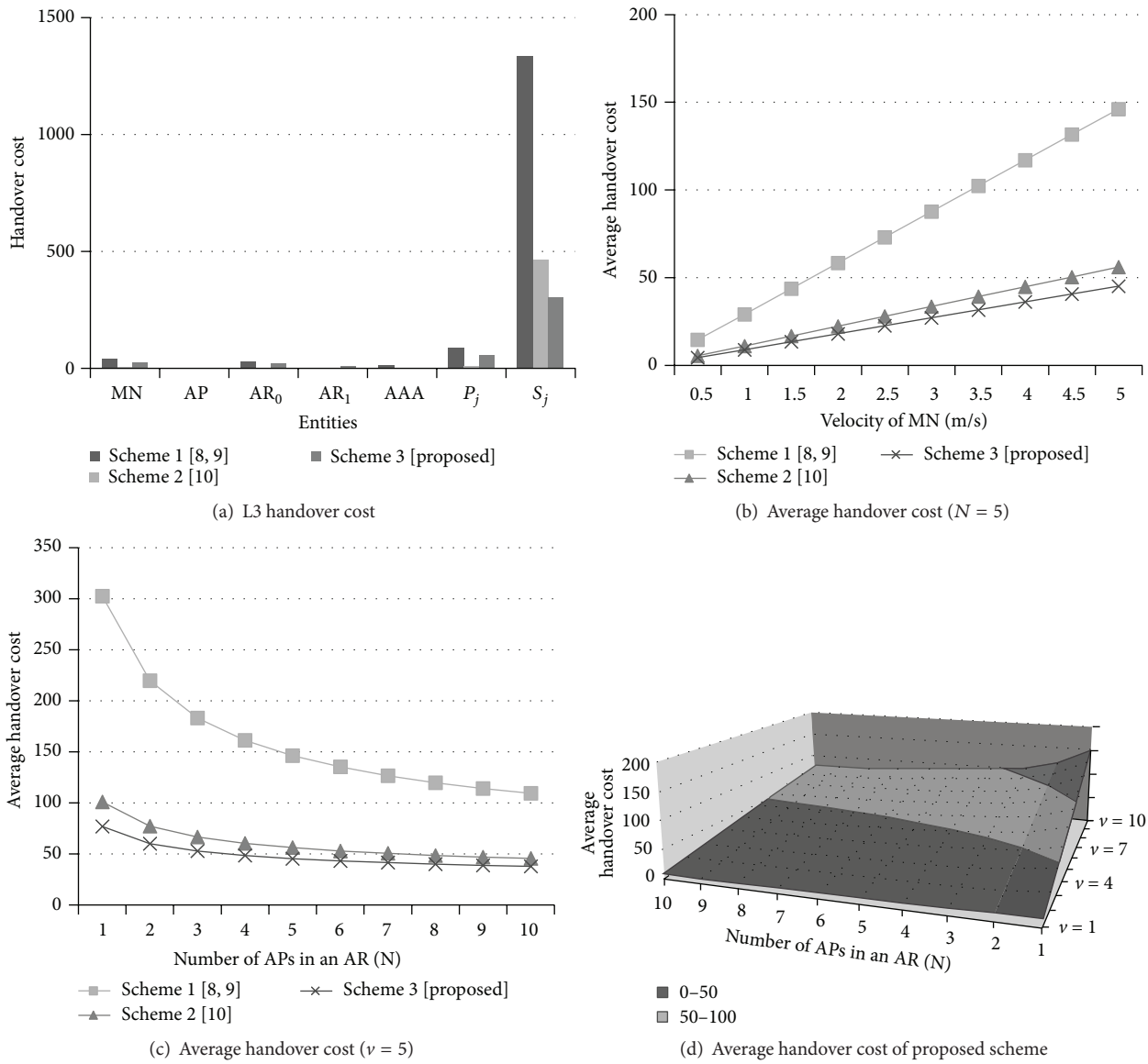
$$P_j = \sum_{i \in Q} a_{ji} P_{ji}, \quad \text{where } Q = \{MN, AP, AR_0, AR_1, AAA\}$$
$$S_j = C_{\text{hop}} \left[C_{\text{wireless}} + C_{\text{wired}} \left(b_{j1} + b_{j2} D_{\text{AP-AAA}} + b_{j3} D_{\text{AP-AR}} \right) \right]. \tag{17}$$

The handover cost of each scheme evaluated according to Table 2 is shown in Figure 6. Figure 6(a) compares the L3 handover costs of the three schemes. It can be observed that the main contributor to the handover cost is the signaling cost, S_j, and the handover cost of the previous schemes is larger than that of the proposed scheme as a result in the difference of when the interaction between the MN and AAA is required. Figure 6(b) shows the average handover cost per MN as the average velocity of the MN increases. The density of MN, p, is set to 0.0002, the number of APs in an AR, N, is set to 5, and the velocity of an MN varies from 0.1 m/s to 5 m/s. The average handover cost for three schemes increases as the velocity increases. Figure 6(c) shows the impact the number of APs in an AR has on the average handover cost per MN. The density of MN, p, is set to 0.0002, and the velocity of an MN, v, is set to 5. The average handover cost decreases as the number of APs in an AR increases.

As we can see from Figures 6(a), 6(b), and 6(c), the proposed scheme is much more or slightly efficient than the previous schemes. Figure 6(d) shows the impacts that the velocity of MN and the number of APs in an AR have on the average handover cost for the proposed scheme. The average handover cost increases rapidly as the velocity of MN increases. However, the average handover cost decreases gradually as the number of APs in an AR increases. Therefore, the velocity of MN, rather than the number of APs in an AR, is a more important factor to consider in order to achieve an efficient handover.

6. Conclusions

We have designed a key management and security scheme to enhance L2/L3 handover security and to reduce the authentication delay induced by the L3 handover. The proposed scheme is based on the original IEEE 802.11-based FMIPv6 where, first, based on the security assumptions, an initial network access protocol has been proposed to bootstrap the security associations among the network entities. Second, a cross-layer key management process has been introduced to integrate the L2 key with the L3 key. Namely, the L3 key can be judiciously employed to derive the L2 key, so that the time-consuming IEEE 802.1x-EAP authentication with the AAA can be skipped. Third, a method for protecting the seven L3 signaling messages has been proposed, as well as a scheme to securely transport the L3 key to the target AR. In particular, the case of a compromised L3 key has been considered for which even though the L3 key at the subnet of the current AR is compromised, an adversary with the compromised L3 key cannot perform any kind of redirection attack. In other words, a domino effect can be suppressed. FMIPv6 over IEEE 802.11 is followed by the MIPv6 BU (Binding Update) protocol which involves an interaction with the AAA of the MSP. In the integrated scenario of MIPv6 bootstrapping, the MSP plays the role of the NSP, while the MSP and NSP are two distinct service providers in the split scenario. As a follow-up to the current research, the AAA issues for security and billing will be more investigated, considering both the split and integrated scenarios for MIPv6 bootstrapping.



(a) L3 handover cost

(b) Average handover cost ($N = 5$)

(c) Average handover cost ($v = 5$)

(d) Average handover cost of proposed scheme

Figure 6: Numerical Results.

Notations

$MAC(K)$:	Message authentication code computed over all preceding message fields using a symmetric key K
$[m]_K$:	Encryption of m using symmetric key K
$kdf(\cdot)$:	Key derivation function
R_X:	Random number generated by X (X = MN, 0 for AR_0, 1 for AR_1)
$Nonce$:	Nonce parameter
$h(\cdot)$:	One-way hash function
$h_{64}(\cdot)$:	64-bit truncation from the output of $h(\cdot)$
K_i:	L3 key shared between MN and AR_i
PMK_i:	L2 key shared between MN and AP_i
PK_X, SK_X:	A pair of public and private keys of X used for the signature
ePK_X, eSK_X:	A pair of public and private keys of X used for the encryption
$Sig(SK_X)$:	A digital signature based on the signing private key SK_X covering all preceding message fields
$[m]ePK_X$:	Encryption of m with the public key ePK_X of X (X = MN, 0 for AR_0, 1 for AR_1).

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Employment Contract based Master Degree Program for Information Security supervised by the KISA (Korea Internet Security Agency) and also supported by the MSIP (Ministry of Science, ICT

and Future Planning), Republic of Korea, under the CPRC (Communications Policy Research Center) Support Program supervised by the KCA (Korea Communications Agency) (KCA-2013-003).

References

[1] R. Koodli, "Mobile IPv6 fast handovers," RFC 5268, 2008.

[2] C. Perkins, D. Johnson, and J. Arkko, "Mobility support in IPv6," RFC 6725, 2011.

[3] IEEE 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard, 2012.

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," RFC 3748, 2004.

[5] P. McCann, "Mobile IPv6 fast handovers for 802.11 networks," RFC 4260, 2005.

[6] Y. Song, M. Liu, Z. Li, and Q. Li, "Handover latency of predictive FMIPv6 in IEEE 802.11 WLANs: a cross layer perspective," in *Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09)*, pp. 1–6, San Francisco, Calif, USA, August 2009.

[7] M. Alnas, I. Awan, and R. D. W. Holton, "Performance evaluation of fast handover in mobile IPv6 based on link-layer information," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1644–1650, 2010.

[8] J. Kempf and R. Koodli, "Distributing a symmetric fast mobile IPv6 handover key using secure neighbor discovery," RFC 5269, 2008.

[9] C.-S. Park, "Security-enhanced fast mobile IPv6 handover," *IEICE Transactions on Communications*, vol. E93-B, no. 1, pp. 178–181, 2010.

[10] J. Choi and S. Jung, "An integrated handover authentication for FMIPv6 over heterogeneous access link technologies," *Wireless Personal Communications*, vol. 71, no. 2, pp. 839–856, 2013.

[11] L. Xu, Y. He, X. Chen, and X. Huang, "Ticket-based handoff authentication for wireless mesh networks," *Computer Networks*, vol. 73, pp. 185–194, 2014.

[12] R. Singh and T. P. Sharma, "A key hiding communication scheme for enhancing the wireless LAN security," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1145–1165, 2014.

[13] X. Li, F. Bao, S. Li, and J. Ma, "FLAP: An efficient WLAN initial access authentication protocol," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 488–497, 2014.

[14] I. You, K. Sakurai, and Y. Hori, "A security analysis on Kempf-Koodli's security scheme for fast Mobile IPv6," *IEICE Transactions on Communications*, vol. 92, no. 6, pp. 2287–2290, 2009.

[15] K. Chowdhury and A. Yegin, "Mobile IPv6 (MIPv6) bootstrapping for the integrated scenario," RFC 6621, 2012.

[16] G. Li, J. Ma, Q. Jiang, and X. Chen, "A novel re-authentication scheme based on tickets in wireless local area networks," *Journal of Parallel and Distributed Computing*, vol. 71, no. 7, pp. 906–914, 2011.